『セキュリティホールに関する法律の諸外国調査』報告書

付録　B　各国報告書日本語訳

B－１　アメリカ合衆国　報告書日本語訳

B－２　カナダ　報告書日本語訳

B－３　フランス　報告書日本語訳

B－４　英国　報告書日本語訳

B－５　ドイツ　報告書日本語訳

B－６　大韓民国　報告書日本語訳

（余白）

『セキュリティホールに関する法律の諸外国調査』報告書

付録　Ｂ－１

アメリカ合衆国　報告書日本語訳

（余白）

アメリカ合衆国における情報セキュリティに関する責任

日本国経済省に対する最終報告書

英語版　2003 年 6 月 30 日

日本語版　2003 年 8 月 29 日

英語版：

テンプル大学ロースクール教授
アメリア・ボス

サイラント・インク
ヴァイス・プレジデント
ジョエル・ロスマン

ジョン・スタンレーP.A.
カリフォルニア州弁護士
ジョン・スタンレー

インフォセック・ロー・グループ
社長兼 CEO
カリフォルニア州弁護士
ステファン・ウー

アメリカ合衆国における情報セキュリティに関する責任[1]

第１章　プロジェクトの概要

本調査プロジェクトの目的は、委託者である経済産業省に、コンピュータネットワークセキュリティの脆弱性に起因する問題に関連する米国の制定法、行政規制、判例法及び諸ガイドラインに関する情報を提供することである。本調査は、民事法、刑事法及び行政法を対象とする。経済産業省は、本調査プロジェクトを通じて、米国を含む諸外国のネットワークセキュリティの脆弱性に対する諸規制や諸基準の概要を明らかにし、比較法的検討を行うものである。本調査報告書は、日本国におけるネットワークセキュリティの責任に関する法制定の検討の一助となるべく経済産業省の調査に用いられるものである。本調査報告書は、米国における情報セキュリティに関する責任につき、連邦法及び州法の概略を説明し、併せて、2003 年 4 月 23 日付けの共通質問状に回答するものである。

本最終調査報告書を通じて、報告者らは、下記仮設事例に適用しうる法律につき説明を試みた。すなわち、ある会社が、別の会社を相手取り、連邦裁判所または州裁判所に訴訟を提起したと仮定する。原告は、そのコンピュータシステムがインターネットを経由して SQL スラマーワーム（以下「スラマー」という。）に攻撃されたが、被告のコンピュータシステムが攻撃の原因であると主張した。但し、原告は、被告会社のシステムがそれ自体被害者であったことも認めている。それにもかかわらず、原告は、被告がスラマーワームの拡散を防ぐ手立てを講じなかったことがスラマーワームを拡散させ、ひいては原告のコンピュータシステムに感染させた主張している。情報セキュリティ攻撃の犠牲者が、感染後の拡散を防ぐ措置を取らず、他者に拡散させて犠牲者とし、損害を被らせることは、しばしば「下流責任(downstream　liability)」と称される。

これに対して、被告は、スラマーの制作者に対して、第三者引き込み訴訟を提起する(制作者が特定できたと仮定した場合)。被告は、制作者に対し、寄与分の請求または損害の填補を主張する。原告もまた、引込第三当事者である制作者に対して、訴訟を提起する。本最終調査報告書の問うているところは、このような仮設事例において、被告や第三者である制作者に対して、どのような法的請求をすることができるか、である。米国調査チームは、本最終調査報告書が、このような問題に対する日本法の解釈の一助となり、また情報セキュリティ責任に関する新たな法制定の際の一助となることを願っている。

[1] [訳者注]オリジナル版には相当数の脚注が付されておりますが、そのほとんどが出典紹介であることから、これらはオリジナル英語版を参照下さい。

第２章　アメリカ合衆国における情報セキュリティに関する責任の概要

本章は、米国において連邦レベルまたは州レベルでの情報セキュリティ違反または事故に伴う責任を決定する際に適用される法律の概要を示すものである。これらの法律のうちで情報セキュリティの問題のみを対象とするものは殆ど存在せず、むしろこれらの殆どはかかる場面に適用される責任に関するより一般的なルールを規定する法律である。適用されうる法律は３つの主要なカテゴリーに分類できる。すなわち、不法行為法、制定法及び契約法である。本章 A 乃至 C は、これらの各法分類に従ってそれぞれのカテゴリーを説明するものである。本章 D は、ガイドラインの説明である。ここで言及されているガイドラインは、それ自体としては法律としての拘束力はないが、適切な行動基準の証拠となりうる点で関連性があり、また契約に盛り込む場合にも関連性があるといえる。

なお本章の説明は、インターネットを含むコンピュータネットワークの利用に起因して生じるセキュリティ違反が生じた場合に特に問題となる責任形態のうちの主要なものに限定されざるを得ないことに留意していただきたい。本報告書は、コンピュータネットワークの利用に伴い発生するその他の責任形態を議論するものではない。例えば、活字媒体で発行されることが容易な情報につき、単にウェブサイトという手段のみを用いて掲載されたからといって、そこで生じる名誉毀損(defamation)や不実表示(misrepresentation)の問題を議論するものではない。このような事案には、活字媒体に関する伝統的な法律分析が当てはまるのであり、ここでかかる分析を繰り返しても実益に乏しいと考える。最後に、本プロジェクトは情報セキュリティを確保するために適切な行動を取らなかった私人の責任に言及するものであり、政府機関等の責任に言及するものではない。

A.　不法行為法

不法行為法が救済するのは、契約違反以外の私人による違法行為または私人の権利侵害である。不法行為法に関する本節は、第１章記載のスラマー事件を基にした訴訟に関する設例で取り上げられうる不法行為に関する幾つかの請求原因を列挙するものである。

１．　過失責任

情報セキュリティ違反に起因する損害賠償を求める原告は、かかる損害に対し作為または不作為により故意によらず貢献した者に対し、しばしば過失責任を主張する。例えば、過失及び法律上の過失（negligence per se）は、いずれも著名なセキュリティ違反事件であるストーレンワーク対トライウエスト・ヘルスケア・アライアンス事件（民事事件番号 03 0185 PHX SRB、2003 年 1 月 28 日提訴）の請求原因である（訴状は、被告が事務所のセキュリティに関して、過失により事務所に侵入を許し原告の健康保険に関する極秘情報が入ったハードディスクドライブを物理的に盗まれたことの責任を主張している。)。

米国においては、過失責任は州法の問題である。州法においては、下記の本質的な要件を原告が主張することを要求することが一般的である：

1.　被告が原告に対し、注意義務を負っていたこと。原告には、当該法律が保護する身体に対する損害または物に対する損害に対する利害関係があったこと。
2.　被告が注意義務に違反したこと。すなわち、例えば被告が原告に危害が及ぶのを防ぐために合理的な注意を払わなかった場合など、被告の行為が法律で規定された行動基準を下回ったこと。
3.　被告の行為により、原告に損害がもたらされたこと。被告の行為は、原告が被った被害と事実上の因果関係（ actual cause）がなければならず、同時に、法的原因(legal cause)または主原因(proximate cause)でなければならない。

過失の概念は以下のように概括されている。すなわち、「コモンローの注意義務は一般に、通常の合理的かつ思慮深い人が同一または類似の状況に置かれた場合に行使し、または行使するのが通例である程度の注意義務を要求している。」

過失責任に関する訴訟で、裁判所が適用する注意義務の基準の根拠は様々である。それ以前の裁判例に依拠することもあれば、特に過失責任事案に適用される注意義務の基準や過失責任の請求において裁判所が適切な注意義務の基準として採用したより一般的な行為基準を示す制定法や行政規制に依拠することもある。判例法、制定法または行政規制がない場合には、裁判所は証拠を採用し、当該事案の事実関係に適用すべき注意義務の基準を決定する。

裁判所が過失責任に関する注意義務の基準として採用していた基準が制定法または行政規制で採用された場合、かかる制定法または行政規制の違反は、「法律上当然の過失」(negligence per se)と呼ばれる。このような法理に基づき、裁判所は、医療情報や金融情報の過失による開示に関する過失責任の有無につき判断するにあたり、注意義務の判断基準として連邦健康保険継続責任法（Federal Health Insurance Portability and Accountability Act）(“HIPAA 法”)あるいはグラム－リーチ・ブライリー金融サービス近代化法（“ GLBA 法 ”）に依拠することがありうる。裁判所がこれらの制定法の注意義務の基準を採用する場合、または行政規制がこららの制定法に従って施行される場合、HIPAA 法または GLBA 法（またはこれらを解釈した行政規制）違反は、法律上当然の過失と見なされる可能性がある。しかしながら、報告者らは、私人による民事訴訟において HIPAA 法または GLBA 法違反が法律上当然の過失とされた裁判例を知らない。

報告者らは、第 1 章記載のスラマー設例において自己のシステムを通じてウィルスを他者に流布してしまった被告に対して主張される主要な請求原因の一つが過失責任の主張であると考えている。なぜなら、過失責任は、誤った行為をした者がかかる誤った行為をしたことにつき責任成立のために現実の故意が要求されない非常に限られた請求の一つだからである。被告がパッチの適用を怠ったことその他スラマーの拡散を防止する措置を怠ったことが、原告のシステムへのスラマーの送信をもたらしたのである。原告は、インターネット上で他者が合理的に予見可能な被害を被らないように防止するよう合理的に行動する注意義務が被告にあったと主張することが可能である。被告には、議論はあるが、スラマーの拡散を防止すべくパッチを適用したりソフトウェアを利用することを怠ったという注意義務違反があったといいうる。最後に、原告は自己のシステムに対する損害及び被告のコンピュータシステムから原告のシステムへワームが拡散したことに起因するスラマーに対応するために費やした時間という形で損害を証明することが可能である。

２．厳格責任

厳格責任の法理は、製品の製造者に対し、欠陥品に起因する被害に関して厳格責任を負わせる。「利用者、消費者または彼らに属する物に対して合理的な範囲を逸脱した危険性を有する欠陥状態の製品を販売した者は、それらによりエンドユーザー、消費者または彼らに属する物に生じた物理的損害の責任を負う。」。原告は、セキュリティホールを含むソフトウェアの開発者や販売者に対して厳格責任法理を利用しようと試みることは可能だが、同法理の伝統的適用形態からは、以下の２つの理由により、情報セキュリティの場面でかかる法理を利用することは困難であるといえる。すなわち、有体物が存在しないこと（せいぜいソフトウェアがあるだけである。)、及び、人または物に対する物理的被害の欠如、の理由からである。

しかしながら、近時の判例及び不法行為に関する新リステートメント（第 3 ヴァージョン）の

1998 年製造物責任は、かかる主張が認められる可能性を高めているといえる。製造物に関し、新リステートメントは「有体物」と定義しているが、定義は更に続けて、「本リステートメントのルールを適用することが適切であると考えられる有体物の頒布及び利用と十分に類似している頒布及び利用の状況下での・・・・その他のアイテム」と規定している。判例法はすでにコンピュータソフトウェアが厳格責任法理に照らして製造物と考えることが可能であることを示唆しているおり、リステートメントのコメントは、適切な事案ではこの規定がコンピュータソフトウェアに適用されることを明確に予定している。

セキュリティホールを含むソフトウェアが頒布され、その利用者が被害を受けた場合に、不法行為の厳格責任の法理に依拠する割合が増加する可能性は高いといえる。

3．動産不法侵害（trespass to chattels）

動産不法侵害（trespass to chattels）の法理は、一部のインターネット企業により、これらの企業の企業内ネットワークに情報、すなわちスパムと呼ばれる無断の商用電子メール、を流した外部者に対し、企業が救済を求める際に採用されてきた法理である。害意あるコードその他の侵入行為が損害をもたらし、人々のネットワークの利用を妨げる可能性がある以上、情報セキュリティに対する攻撃に対し、動産不法侵害の法理が主張される可能性はある。

動産不法侵害の法理は、物の占有妨害を含む。動産不法侵害の主張の主たる要素は下記のとおりである。すなわち、

1. ある者が故意に動産を利用し、または干渉すること。
2. 動産が他者の合法な占有下にあること。
3. 当事者の利用または干渉行為が無権限で行われること。
4. 利用または干渉行為により、動産は状態、性質及び価値を損なっていること。

また、動産侵害は、被告が原告の動産につき「占有侵奪」（”dispossession”）行為をした場合にも生ずる。「占有侵奪」とは、被告が行為を行った場合である。

a. 原告の同意なく原告から動産の占有を取得する場合。
b. 詐欺または脅迫により、原告から動産の占有を取得する場合。
c. 原告が当該動産にアクセスすることを妨害する場合。
d.原告の占有中に、当該動産を損壊する場合。
e. 当該動産を法律上の管理化に置くこと。

判例法は、原告が原告の装置の価値の下落、原告のストレージスペースの枯渇、及びコンピュータのプロセス力、原告のサービスの利便性の低下、顧客を助け侵害的通信行為を阻止することに伴う費用、サービス利用を止めた顧客からの逸失利益、及び原告の評判やグッドウィル（顧客吸引力）の低下、を回復できることを示している。

これら全ては、スラマー仮設事例に関連している。従って、筆者らは動産不法侵害法理は、第 1 章仮設事例におけるスラマーの著作者に対する主要な請求の一つであると考えている。スラマーの著作者は、ソフトウェア作成行為及びワーム拡散行為により、許諾なく世界中のコンピュータシステムに故意に干渉し、機能を損なわしめた。システムオペレーターが感染コードを除去するためにシステムをシャットダウンしなければならなかった間、システムの所有者はシステムに対する占有を奪われた。

しかしながら、犠牲となった企業にとり、動産不法侵害の請求を、ワームを拡散した流れの上流にいて下流に拡散した犠牲者に対して主張するのはより困難であろう。その結果、スラマーの拡散を防止する措置を取らなかった不注意な犠牲者は、議論あるところだが、動産不法侵害請求の対象外と考えられる。

４．予測される将来の契約関係に対する妨害行為(Interference with Prospective Contractual Relations)

契約関係に対する妨害行為を含む不法行為は、例えばサービスを拒否せしめるような攻撃や害意あるコードを利用するなどして、攻撃者が電子商取引サイトを利用不能にした場合などに適用されうる。契約履行に対する故意の妨害行為に関する不法行為は、顧客に対し約束しているサービスを提供することを妨害する攻撃行為が行われた場合に適用されうる。攻撃者は、サービスを受けることを期待していた顧客またはサービスを提供しようとしていたサイトのいずれかに対して責任を負う可能性がある。予測される契約関係に対する妨害行為という不法行為類型は、原告のシステムに対する攻撃により電子商取引サイトがオンラインで新しい顧客を確保することが妨害され、新たな契約締結が妨害された場合などに適用される可能性がある。

既に存在する契約に対する妨害という不法行為は、以下の要件のもとに成立する。すなわち、
1. 契約の履行を故意または不適切な行為により妨害すること。
2. 原告と第三者との間に契約関係があること。
3. 被告は、契約当事者の一方が契約を履行しないように誘引、その他の履行しない原因を作出し、当事者による契約履行を妨げ、または契約の履行により大きなコストその他の負担がかかるようにしたこと。
4. 被告の行為の結果、原告が金銭的損害を被ったこと。

予想される将来の契約関係に対する妨害という不法行為は、以下の要件のもとに成立する。すなわち、
1. 予想される将来の契約関係を、故意または不適切な行為により妨害すること。
2. 妨害行為が、(a) 第三者をして予想される契約を締結せずまたは関係を継続しないことに関し誘引その他の原因を作出し、または(b)相手方をして予想される関係を形成し継続することを妨害すること。
3. 被告の行為の結果、原告が当該関係が形成されなかったことに伴う金銭的損害を被ったこと。

かかる行為は、故意かつ「不適切」でなければならない。

スラマー仮設事例では、SQL データベースに依拠して電子商取引サイトを運営していた原告は、スラマーの作者に対して、スラマーの作者がビジネスをシャットダウンさせる目的でワームを流布したことを証明できる限りにおいて、オンラインビジネスに対する妨害行為に対する請求が可能と考えられる。場合によってはスラマーは既存の顧客に対するサービスの提供を妨害し、また場合によってはスラマーは新しい顧客から注文を受け付け契約を締結することを妨害した。スラマーの作者は、これらのサイトには顧客との間に契約があること、または新たな顧客との新規契約の試みがあることを知っていたはずである。従って、スラマーによる問題のために契約が実現できなかった当事者は、スラマーの作者に対し、既存の契約関係に対する妨害行為または潜在的契約関係に対する妨害行為を主張できる。

しかしながら、スラマーの犠牲者にとって拡散の流れの上流にいる他の犠牲者に対して請求することは困難であろう。妨害行為の不法行為の主張にとり、ここでも主観的意図は本質的要素となっているのである。従って、下流の当事者の契約を妨害する意図を有さずに、単に彼らの

システムがスラマーを下流の犠牲者に拡散するに任せた不作為による妨害行為に従事した上流の犠牲者は、このような不法行為類型の範疇外にある可能性が高い。

５．寄与分及び求償(Contribution and Indemnity)

寄与分及び求償は、被告が第三者や他の当事者に責任を転嫁するために用いられる法理である。例えば過失事案では、被告は第三者に対し、原告の損害のうちかかる第三者の行為に起因する割合につき、かかる第三者が損害賠償することを確認する主張をすることが考えられる。求償は寄与分とは異なる。すなわち、求償においては、法はある不法行為の被告が他の不法行為の被告よりもはるかに責任が大きい場合に、かかる責任の大きな被告に対し原告の損害額全額の支払義務を認めるものである。第 1 章記載のスラマー仮設事例において、被告は寄与分を回復できる可能性が高く、また場合によっては原告に対し責任を負うスラマーの作者に対し求償できる可能性がある。なぜなら、スラマーの作者こそが最初に害意あるコードを書き、拡散せしめた張本人だからである。

６．不法行為に関するその他の問題

情報セキュリティが攻撃を受けた場合、場合によってはその他の不法行為の請求原因が発生することがある。かかる状況は下記を含む。

- 転換（Conversion）（被告の攻撃または害意あるコードが原告のシステムに大きな損害を与えシステム全体の価値を賠償することが公平と考えられる場合に、システムへの損害をシステム全体の価値に置き換えて賠償を認めること）
- プライバシー侵害（実際には不法行為の 4 類型から成り、そのうちの 2 類型が関連している。）
- 詐欺（金銭または物を取得するために害意あるコミュニケーションまたは電子情報の改ざんをすることも詐欺の一類型である。）
- 忠実義務違反（会社の株主は、取締役や執行役員に対し、情報セキュリティに対する注意の欠如が会社に被害を生ぜしめたと主張することが予想される。）
- 故意による精神的損害の惹起行為（コンピュータシステムに対するハッカーの攻撃は、故意による精神的損害の惹起行為を構成する行為の一つと言いうる。）

B. 制定法/行政規制法

ディジタル/リーガル・セキュリティ/ライアビリティ問題につき特に明記した主要な連邦制定法は２つある。一つは、コンピュータ詐欺及び不正利用防止法（The Computor Fraud and Abuse Act (“CFAA”)）(18 USC §130)である。

1. コンピュータ詐欺及び不正利用防止法（CFAA 法）

CFAA 法はコンピュータ関連の刑事犯罪その他の不正行為に関する予防、訴追及び救済に関して定める最も重要な連邦制定法である。CFAA 法は、同法違反による損害に対する私訴の権利を規定している。その結果、CFAA 法に基づく法的主張や訴えは、政府または私人たる原告により提起されうる。

CFAA 法は主として下記を禁止している。

- 故意に権限なくまたは権限を逸脱してコンピュータにアクセスし、州をまたがる交信または国際間の交信の手段としての「保護されたコンピュータ」から、または金融機関やクレジットカード発行人のファイナンスレコードから、情報を取得すること。

- (1)米国政府内部またはエージェントの非公共のコンピュータまたは非政府団体と政府が共有している非公共のコンピュータに故意、無権限でアクセスし、(2)当該違反が標的となったコンピュータの政府による利用に影響を及ぼす場合に、かかる政府のコンピュータをハッキングすること。
- 「詐欺」の計画を進める目的でコンピュータを使用すること。
- 保護されたコンピュータに「損害」を生ぜしめること。
- コンピュータにアクセスするために利用される情報やパスワードを無権限で取引すること。
- 保護されたコンピュータに危害を加えるとの威嚇を、州を越えてまたは国際間の取引において交信し、金員を強要すること。

損害発生に関する同法§1030(a)(5)は、スラマー仮設事例及び本調査報告プロジェクトに最も関連する規定といえる。同法中「損害」は、「コンピュータ」上の「データ、プログラム、システムまたは情報の統合性や入手可能性に対するあらゆる危害」と定義されている。同条項は以下の 3 類型の行為を禁止している。

- 第一に、意図的にプログラム、情報、コードまたはコマンドを送信し、その結果保護されたコンピュータに権限なく意図的に損害を生ぜしめること。
- 第二に、無権限で保護されたコンピュータに故意にアクセスし、その結果向う見ずにも当該コンピュータに損害を生ぜしめること。ここで要求される故意はコンピュータに対するアクセスに対するものであり、損害にいたる因果関係に対するものではない。
- 第三に、「意図的に無権限で保護されたコンピュータにアクセスし、その結果損害を生ぜしめる」者の行為を禁止している。第二と第三の唯一の違いは、当該行為が向う見ず（reckless）になされることは、加害行為を立証する上では必要ないことがある。要件がより緩やかであることに対応して最高刑罰も低くなっている。

スラマー仮設事例において、スラマーの作者は、議論の余地はあるが、上記第一乃至第三の行為をいずれも行っていたといえ、かかる作者の行為がスラマーの犠牲者のコンピュータシステムに損害を及ぼしたといえる。条文のうち「プログラム、情報、コードまたはコマンドを送信」により損害を生ぜしめることの禁止を規定する部分に、スラマーワームの作者の行為がそのまま該当するといえる。最後に、スラマーワームは犠牲者のコンピュータシステムに侵入したのであるから、議論の余地はあるが、第二及び第三に違反して犠牲者のシステムに「アクセス」したものといえる。かかるコンテクストから、意図的な行為の要件は、被告が原告や犠牲者に損害を加える意図を実際に有せずに行為をした場合であっても、被告が意図的と主張されるような行為をすれば充足されるとの意味であると解釈される可能性が高い。

2. 電子コミュニケーション・プライバシー法(ECPA 法)

ECPA 法は、電子、コンピュータまたはインターネットによる交信を傍受し、利用しまたは開示するといった類の行為を禁止している。ECPA 法はまた、電子交信サービスや交信保存の設備を保護する交信保存法(Stored Communications Act (“SCA 法”))を含んでいる。いずれの法律も同法が禁止する行為により損害が発生した場合に被害者に私訴の権利を付与している。

ECPA 法は、刑事犯罪の以下の 3 つの類型を提供している。

第一に、18 U.S.C. §2511 は、同法の他の条項により特に許容されていない限り、あらゆる「電信、口頭または電子交信」による故意の、無権限な、傍受、利用または開示を禁止している。§2511(1)(a)及び(b)に基づく主張が認められるためには、政府または原告は、下記の 5 要件を示さねばならない。すなわち、被告は(1)故意に、(5)装置を利用した(4)電子更新の(3)内容を(2)自

ら傍受しまたは傍受しようと試み、あるいは他人をして傍受させまたは傍受させようと試みる場合でなければならない。但し、同意その他制定法上の例外がある。「傍受」は、「電子的、機械的またはその他の装置をつかっておこなわれた電信の、電子的な、または口頭の交信の内容を取得すること」と定義されている。

第二に、18 U.S.C. §2512 は、郵便や州際間または国際間商取引を通じて、故意に「主に送信、口頭または電子的コミュニケーションを秘密裡に妨害する目的に資する」装置を送付する行為を刑事犯罪としている。かかる規制はまた、かかる装置の製造、販売及び広告にも広く適用される。

第三に、18 U.S.C. §2701 は以下の者に刑事罰を課している。すなわち、

- 「故意かつ無権限に、電子コミュニケーションのサービスを提供する設備にアクセスする者」
- 「電子的にシステムの中に蓄えられている際に、故意に権限を逸脱してかかる設備にアクセスし、送信または電子的コミュニケーションへのアクセス権を獲得し、変更し、または妨害する者」

本項は、インターネットサービスプロバイダーのシステムへのワームの注入が「アクセス」を構成する限りにおいて、第 1 章で述べたスラマーワームの仮設事例に当てはまる可能性がある。スラマーが ISP のシステムをシャットダウンした限りにおいては既存の蓄えられているコミュニケーションへの権限あるアクセスが妨げられているけれども、蓄えられている伝達記録へのアクセスを刑事犯罪とする本制定法の後半部分は、この仮設事例との関係ではより関係性が希薄といえる。ECPA や SCA の禁止違反に対しては、それが刑事であると否とを問わず、私訴が可能である（ワイアータップ法(The Wiretap Act)（ECPA 法により修正される。）は、これらの救済方法を 18 U.S.C.§ §2520, 2712 において規定している。）。

3. 行政規制分野と情報セキュリティ責任

a. 健康保険継続責任法(HIPAA 法)

健康保険継続責任法（ Health Insurance Portability and Accountability Act）(以下「HIPAA 法」という。）は、特に健康保険企業、ヘルスケアプロバイダー及びヘルスケア情報センター（同法においては「適用機関」という。）によるプライバシー及びセキュリティの取扱いに関して広範な要件を規定したという点で、米国において画期的な事件となる立法である。HIPAA 法によれば、健康情報を維持または送信する適用機関は、以下の目的の資するべく、合理的かつ適切な管理上、技術上及び物理上のセーフガードを維持しなければならない。
（A）情報の統合性及び秘密性を担保する目的、
（B）合理的に予想できる(i)情報のセキュリティまたは統合性に対する脅威または危険、及び、(ii)情報の無権限での使用または開示、から守る目的、
及び、
（C）その他これらの機関の役員や従業員がこれらを遵守することを担保する目的。

HIPAA 法は、健康省長官(the Secretary of Health and Human Services)に対し、ヘルスケアに関する様々な基準（規制一式）を作成することを要求している。これらの基準の一つには、ヘルスケア患者の「個人を特定できる健康情報」のプライバシー保護のためのものであり、健康省（the Department of Health and Human Services(“DHHS”)）は実際に、この点に関する最終的なプライバシー基準を採用している。もう一つの基準は、「保護された電子健康情報」のセキュリティのためのものであり、DHHS により 2003 年 2 月に公布されている。

セキュリティ基準の目的は、保護された電子健康情報の秘密性、統合性及び入手可能性を保護することにある。かかる基準は、適用機関に対し、管理上の、個人の、そして技術上のセキュリティコントロールを導入することを要求している。かかる規制の中で言及されているコントロールの一つは、害意あるソフトウェア（malicious software）に対して予防措置を講じることである。害意あるソフトウェアとは、例えばウィルスのように、システムに危害を与えたり破壊したりする目的のソフトウェアのことをいう。スラマーワームはこの定義の範疇内である。

害意あるソフトウェアに対する防護のためのかかるコントロールを含むことはスラマーワームに対する防護を含むことを意味するが、かかるコントロールを導入しなければならないという絶対的必要条件ではない。このコントロールは、HIPAA 法のセキュリティ基準では、「アドレスで呼び出せる導入仕様」と呼ばれている。HIPAA 法適用機関は、アドレスで呼び出せる導入仕様が保護された電子健康情報のセキュリティへの貢献度という観点から合理的かつ適切であるか分析する。特定のコントロールが適用機関にとり合理的かつ適切な場合、適用機関はかかるコントロールを導入しなければならない。しかしながら、適用機関がかかる特定のコントロールを導入することが合理的かつ適切でないと信じた場合、導入する必要はない。但し、当該機関は、合理的かつ適切でないと信じた理由を書面化しなければならず、また同等の別のコントロールを導入しなければならない。以上にもかかわらず、筆者らは、アンチウィルスソフトが安価で広範に入手可能であることからすれば、HIPAA 法適用機関の相当多くは、害意あるソフトウェアに対するコントロールを導入することが要求されると考える。

HIPAA 法は、DHHS が行政訴訟により、同法違反者に対して民事制裁金を請求できる旨規定している。政府はまた、HIPAA 法に故意に違反した者に対して刑事訴訟を提起することができる。しかしながら、他の多くの法律と異なり、HIPAA 法は違反に対して特段の制定法上の私訴の権利を規定していない。従って、HIPAA 法は、私人が、HIPAA 法適用機関に対し、同法違反を理由に損害賠償請求することを認めていない。これに代わるものとして、HIPAA 法適用機関に対し、同法違反を理由として損害賠償請求する私人は、法律上の過失法理（the doctrine of negligence per se）に依拠しなければならないかもしれない。法律上の過失法理に関しては、前記第 2 章（A）(1)参照のこと。

HIPAA 法は、スラマーワームに関し、下記の点で関連性がある。すなわち、適用機関が害意あるソフトウェアに対して合理的かつ適切なコントロールを導入しなかった場合、DHHS はかかる機関に対し、HIPAA 法の規定に基づき行政訴訟を提起する可能性がある。損害を被った原告が、第 1 章記載のスラマー仮設事例のようにワームを拡散させた HIPAA 法適用機関に対して民事訴訟を提起する場合には、原告は法律上の過失法理に依拠する必要がある。筆者らの意見は、裁判所が HIPAA 法のセキュリティ基準を、スラマーワームを拡散させた適用機関に適用される注意義務の基準として採用し、もって過失責任が明確な可能性となるということが大いにありうるということである。しかしながら、上記のとおり、法律上の過失法理における注意義務の基準として HIPAA 法を援用しようとした判例はまだないものと理解している。

b. 金融情報の保護: グラム・リーチ・ブライリー法

グラム・リーチ・ブライリー法または GLBA 法として知られる 1999 年の金融近代化法(The Financial Modernization Act of 1999)は、「金融機関」に対するプライバシー及びセキュリティに関する要求を規定している。ここに「金融機関」の定義は広範である。これには、「金融商品または金融サービス」を提供する業務に「重要」に携わっている機関を含んでいる。GLBA 法の基本的なポイントは、「各金融機関に対し、顧客のプライバシーを尊重し、顧客の非公開の個人情報のセキュリティと秘密性を守る継続的かつ積極的な義務を課している点」である。

一般に、金融機関は顧客の「非公開の個人情報」を「無関係の第三者」に開示してはならない。GLBA 法は、金融機関に対し、プライバシーポリシーとプライバシーの取扱いに関し通知することを要求している。金融機関は、プライバシー通知に従った開示に対して顧客が明確に反対の意思表示しない限り、顧客の非公開情報を無関係の第三者に開示することがありうる。GLBA 法は、様々な連邦または州行政機関に対し、同法の趣旨を実現するための規則を制定する責任と権限を与えている。これらの規則は、GLBA 法により課せられているプライバシー及びセキュリティの要求を肉付けしている。

GLBA 法を導入するために連邦または州行政機関により制定された様々な規則の詳細を仔細に検討することは、本報告書の範疇を越える。規定の仕方は様々であるが、かかる規則は、金融機関に対し、合理的に予想される脅威から記録のセキュリティを守ることを義務付けているということを指摘すれば本稿では十分である。スラマーワームは、その他の害意あるソフトウェアと同様、合理的に予想される脅威であるから、連邦または州行政機関は、スラマーワームに対してセーフガードを取ることを怠り他者に対し同ワームが拡散するがままにした金融機関に対し、行政訴訟を提起することができる立場にあると言いうる。

HIPAA 法同様、GLBA 法は私訴の権利に関しては明記していない。従って、金融機関のコンピュータシステムから感染させられたスラマーワームにより攻撃を受けた者は、GLBA 法そのものを用いて、当該金融機関による GLBA 法違反を主張できない。これに代わって原告は、ワームの拡散の防止を怠ったことに関して法律上の過失があったか否かの分析にあたり、GLBA 法及び同法に基づき公布された規則が金融機関に課される注意義務を構成すると解すべきであることを、裁判所に説得する必要があると思われる。いずれにせよ、HIPAA 法の解説部分いおいて言及したように、金融機関が情報セキュリティ違反の責任を負うか否かの決定にあたり、法律上の過失法理に基づき金融機関の行為に対して GLBA 法を適用した判例はまだないものと理解している。

c. サーバネス・オクスレー法(Sarbanes-Oxley Act)

サーバネス・オクスレー法は、ある上場企業による虚偽取引に関する不正行為の結果米国を襲った金融及び行政のスキャンダルの波を端緒として制定された。米国企業や会計事務所に対するより厳しい監督の必要性が叫ばれた。かかる法案の各条項の分析は本稿の意図するところではないが、数点説明をすべき点がある。まず第一に、同法 103 条は、上場企業会計監視委員会の設置を義務付け、7 年間、監査人の監査報告書の結果を基礎付ける会計監査のために提出された全ての書類その他の関連資料を保持することを義務付けた。監査人が電子的形式で保持する情報への攻撃またはその統合性を維持することの懈怠は、責任を発生させうる。

更に、同法は、証券取引委員会が、金融顧客に対するデータの規則的な保存を要求する規制 17 C.F.R.§ 240.17a-4 を制定することを命じている。行政機関は、「変質しないメディア」に 7 年間電子メールを保存することが義務付けられている。この義務は非常な難題であり、これらの記録に対する攻撃または統合的保存の懈怠は、当該機関の責任を発生させる可能性がある。

最後に、同法第 404 条は、役員と経営幹部に対し、正確な「ファイナンシャル・レポート」を行うことを可能とする「内部的コントロール」及び「手続き」を導入することを義務付けている。従って、識者の中には、本条が黙示的に入念かつ書面化された情報セキュリティ制度を設立することを義務付け、上場会社の役員が個人的に責任を負うものであると主張する者もいる。同法案が施行されて間もないこと、つとに有名なその複雑な内容及び判例法の欠如からすれば、本法案に関しては、将来の発展を待つという以上には論じることは現状では困難である。

d. 強制的に報告を義務付ける法律

米国における近時の傾向は、顧客の個人情報を有する企業や行政機関がシステムのセキュリティに関して危険を感知した場合、かかる顧客にインシデントの報告をすることを義務付ける法律が増えていることである。これらの法律の趣旨は、個人情報の記録が危険にさらされた者が情報を盗んだ者を突き止めることを容易にすることにある。このような法律のうち最も著名なものは、カリフォルニア州の上院法案第 1386 号(SB1386)であり、これはカリフォルニア民法第 1798.29 条、1798.82 条及び 1798.84 条として成文化されている。SB1386 は、2003 年 7 月 1 日に施行された。

SB1386 に類似する法案は米国上院においても紹介されている。加えて SB1386 は、他の法律とも類似している。例えば、金融機関は特定の疑わしい行動を報告する義務を負う。また、州法の中には州検察による起訴に備えて、サイバー犯罪を州検察に報告することを義務付けるものがある。

SB1386 は、コンピュータ化された暗号化されていないデータでカリフォルニア州住民の特定の個人情報を含むものを所持またはライセンスする行政機関やカリフォルニアで事業を行う企業に影響を与えるものである。SB1386 は、かかる行政機関や企業に対し、個人情報に対するセキュリティが破られ、かかる情報が無権限の第三者に取得されたと合理的に考えられる場合には、カリフォルニア住民に通知することを義務付けている。同法案は、法執行機関が刑事訴追のための調査が必要と判断した場合には、同法案に基づく通知義務の履行を遅らせることができるとしている。同法は、違反により損害を被った顧客に対し、同損害の賠償を求める民事訴訟を提起することを認めている。

これらの制定法は、スラマーワームを拡散したといった行為に対する責任を規定していない。代わりに、特定の類型の違反があった場合に報告義務を課するという二次的な義務を規定している。従って、これらの制定法上責任が発生するのは、インシデントの報告を懈怠した場合に限られる。

e. カリフォルニア州民法第 1798.85 条

カリフォルニア州民法第 1798.85 条は、カリフォルニア州民の社会保険番号の利用につき規定している。同条によれば、(州及び地方行政機関を除く)全ての個人や機関は、特定の方法で個人の社会保険番号を表示することを禁じられている。ここで特に注目すべきは、同法が「安全」な方法で「暗号化」しない限り、インターネットを介して社会保険番号を送付することを禁止していることである。「安全」につき同法は定義をしていない。立法者は、同条違反に対し特段のペナルティーを課していない。従って、政府の法執行機関は対応が定かではなく、同条に基づく民事訴訟においては、かかる条項違反が法律上の過失を構成すると主張されると考えられる。

同条は、社会保険番号の意図的なまたは意図しない開示につき規定していることから、同条は、ウィルスやワームに対する保護というよりもむしろ社会保険番号を保持するビジネスや社会保険番号を保護するための方策に関して適用される。従って、本条はスラマー仮設事例には該当しないが、その他の情報セキュリティ攻撃には適用される可能性がある。

f. その他の制定法

情報セキュリティ攻撃に関する責任の根拠となる制定法としては、以上の他に、下記のようなものがある。

- 営業秘密を盗むことを禁止する経済スパイ行為防止法(The Economic Espionage Act)
- ウェブサイト運営者に対し「児童から収集した個人情報の秘密性、安全性、及び統合性を守るために必要な合理的手続きを設定維持」することを義務付ける児童オンラインプライバシー保護法(The Children's Online Privacy Protection Act of 1998)
- 連邦取引委員会法及び不公正及び欺瞞的取引禁止に関する諸法律
- 18 U.S.C. §1029(アクセスデヴァイス詐欺)
- コンピュータ犯罪に関する諸州法

但し、これらの制定法の全てがスラマー仮設事例に適用されうるわけではない。

C. 契約法

契約とは、一般に 2 以上の当事者間で特定の事柄に関して法律上の義務を創設する性質を有する合意である。契約の一方当事者が契約により義務付けられている合意事項を履行しない場合には、法律は損害を受けた当事者に救済を提供する。

原告が被告に対して契約違反を主張するには、原告は下記を主張しなければならない。

1. 原告及び被告が有効な契約を締結したこと。
2. 被告が契約で合意した保証または義務規定に違反したこと。
3. 原告が契約上の義務を履行したこと、または少なくとも履行の提供をしたこと。
4. 被告の義務不履行の結果、原告が損害を被ったこと。

情報セキュリティに対する攻撃の犠牲になった当事者は、契約法理を用い、被告が原告に対する契約上の義務に違反したと主張して、攻撃を行った者、攻撃を許容した者、攻撃を阻止することを怠った者等の責任を追及することが考えられる。かかる場合、原告は、被告が原告との間に、被告が(1)原告のシステムを攻撃したり、同システムに損害を生ぜしめないようにすること、または(2)原告に対する攻撃を防御することにつき、契約を締結していたことを示さねばならない。前者の契約違反の主張の例としては、顧客に提供されるソフトウェアに害意あるコードが含まれないようにするソフトウェアベンダーの義務がありうる。後者の契約違反の主張の例としては、ネットワークに対する危害から原告のシステムを守るためにベンダーが用いられている場合の、原告のネットワークに対する危害を防止する管理されたセキュリティベンダーの義務がある。

情報セキュリティ攻撃の犠牲者に対して契約責任を負う潜在的可能性がある当事者には、以下が含まれる。

- ハードウェアまたはソフトウェア製造業者または開発者（原告が利用している被告のハードウェアまたはソフトウェアに脆弱性がある場合）、
- コンサルタント、システムインテグレーター、ディストリビューター、リテイラーその他原告に脆弱性に関する技術を推奨または提供しているベンダー、
- セキュリティを評価したり、情報セキュリティの脆弱性を修正するために雇われたコンサルタント、
- 脆弱性を発見するために採用された監査人、
- 原告に対する情報セキュリティ攻撃を防止しまたはこれに対する対応を担当する管理されたセキュリティプロバイダー、
- 原告のアプリケーションをアップデートしパッチを施すことを担当してきたアプリケーションサービスプロバイダーまたは外注先のベンダー、

- 原告のシステムまたはアプリケーションサーバーをホストしているホスティング会社、
- 攻撃を許容していたり阻止しなかったシステムやソフトウェアに関するインタネットサービスプロバイダー、及び
- 脆弱性を発見したが、原告、ベンダーまたは一般の人々の注意を喚起しなかった者で、開示義務があると見なされる者。

情報セキュリティ責任を基礎とする契約違反事件の主要な争点は下記を含む。

- 契約の適切な解釈から、被告は原告に対して、原告に対する情報セキュリティ攻撃を阻止したり、予防する義務を負っているか。
- 被告は、情報セキュリティに関して原告に対して負っている契約上の義務を適切に履行したか。
- 被告による潜在的違反行為は、被告による義務の履行を前提条件とした条項を原告が履行しないことにより、免責されるか。例えば、被告が原告に特定の情報セキュリティサービスを提供する契約において､原告自身にも内部的なセキュリティに関する義務が規定され、原告がかかる義務を履行することが被告が義務を履行する上で必要な場合がある。原告がその責任を全うしないことにより重大な契約違反をした場合、被告による契約違反を免責するとみなされる可能性がある。
- 損害の発生要件や損害額を限定する合意条項は執行可能(enforceable)か。
- 原告の主張は、契約上規定されている仲裁に付さなければならないか。

契約法は、コンピュータウィルス、ワームまたはネットワークセキュリティ違反による損害からの救済方法を提供しているが、その射程範囲は狭い。米国の契約法は、一般に契約違反からの救済を(直接の)契約関係にある者(privity)に限定している。当初の契約の当事者でない第三者は、契約当事者でないために契約違反に起因する損害の救済を受けることができない可能性がある。

契約当事者の一方がウィルス、ワームまたはネットワークセキュリティ違反で損害を被った場合の契約違反に関する判決は未だに報告されていないが、似たような事実関係で下された判決が幾つかある。これらの判決は、ネットワークセキュリティに関する契約違反事件がどのように判決されるかに関して類推できるものである。誤作動したソフトウェアに関する契約違反の主張は、ソフトウェアのデザイナーに対してなされてきた。そこでは、かかるソフトウェアを利用していた顧客は、誤作動により損害を被ったという主張がなされた。例えば、ワーナー、ザーロフ、スロトニック、スターン及びアシュケナージ対ルイス事件(*Warner, Zaroff, Slotnick, Stern & Askenazy v. Lewis* (155 Misc. 2d 558 N.Y.S. 2d 960 (Civ. Ct., N.Y. Cty. 1992))において、裁判所は、被告が設計し原告に売却したコンピュータシステムが誤作動し原告のビジネスを妨げた場合に、原告に懲罰賠償を含む損害賠償を認めた。裁判所の認定した事実関係によれば、被告は契約に違反し、提供するソフトウェアプログラムのソースコードに「条件付ステートメント」を含ませ、それにより一定数のオペレーションを行うと自動的にシステムがシャットダウンするように設定された。被告は、ときに「時限爆弾」とも呼ばれるこの条件付ステートメントを、原告から被告に追加のコンピュータサービスを依頼させるようにするために仕込んだことは明らかであった。裁判所は被告の契約違反を認定したことに加え、被告が害意をもってかかる行為をしたことを認定し、制裁を加えるために追加的損害賠償を認めた。

ネットワークセキュリテイに類推できるような判決も出ている。一般的なシナリオとしては、インタネットハッカーの祖先である電話「フリーカー」がある。これは、顧客の電話システムに侵入し、電話回線に接続して、高額な長距離電話をかけてしまうという事例である。かかる電話回線利用料が請求書に記載されると、顧客は一般に、無権限の電話回線利用行為であることを理由

として支払いを拒む。現在まで、このような事案では、裁判所は、かかるセキュリティ違反から防御するに一番適した立場にあった当事者に損害の責任を負わせている。

例えば、アメリカ電信電話会社対ジッフィー・ルーブ・インターナショナル事件（*American Telephone and Telegraph Co. v. Jiffy Lube International, Inc.* (813 F. Supp. 1164 (D. Md. 1993)）では、顧客であったジッフィー・ルーブは、セキュリティコードを入力するだけで同社の電話システムにアクセスし無料で利用できる非公開の電話番号を有していた。裁判所は、ジッフィー・ルーブと長距離電話会社との契約を執行し、ジッフィー・ルーブに回線使用料を支払うよう命じた。

以下の項では、情報セキュリティ違反のコンテクストでどのように契約違反の主張がなされているかを説明する。下記 2 及び 3 における議論は、当該論点を直接判示した判決はないとはいえ、ネットワークセキュリティ攻撃及びソフトウェアの脆弱性のリスクを効果的に管理するために契約が用いられる様々な場合を示している。

1.　ソフトウェアのベンダーの契約責任

契約法は、以下のような理由から、セキュリティの脆弱性を作り出すソフトウェアまたはハードウェアの欠陥に対する実効性のある救済方法といえる。

- 契約法は純粋に経済的損失に対する救済を提供する。不法行為のような他の責任法理は、純粋に経済的損失のみの場合の救済を含まないことがある。また、他の制定法上の救済方法は、セキュリティ違反に起因する損害の賠償を提供していない。
- 契約は当事者間の私的な合意であり、特定の注意義務の程度に関し当事者が自由に決定できる。例えば、インタネットサービスプロバイダーのインターネットサービス契約では通常一定の「サービスレベル」が規定されている。アクセスを一定の要求されているレベルまで提供できなかった場合には、一定の効果が生ずる。不適切なネットワークセキュリティのように近時新たに議論されるに至った責任に関しては、裁判所が損害について責任を振り分けるために参照できる確立された契約上の基準がないかもしれない。契約は、当事者をして、特定の状況下における私的な基準を確立することを可能にしている。
- 契約当事者間では、責任の振り分けは容易である。なぜなら、当事者自らが契約違反につき責任を負う場合を決定しているからである。不法行為や刑事法のような救済理論においては、責任成立のため相当因果関係の立証が必要となる。ネットワークセキュリティ違反事案においては、ハッカーが故意にネットワーク安全保護を破った場合には、相当因果関係が中断されるといわれる可能性がある。しばしば中断原因(intervening cause または superseding cause)として言及されるが、相当因果関係の立証ができないことは、不法行為損害賠償請求または刑事法における私訴に基づく損害賠償請求にとり致命的である。

2.　管理されたセキュリティプロバイダーに外注されたネットワークセキュリティ (Outsourced Network Security with the Managed Security Provider)

ここ数年、ネットワークセキュリティ専門のベンダーが様々な団体に対してセキュリティサービスを提供し始めている。管理されたセキュリティプロバイダーまたは MSP は、一般に顧客から報酬を受けてネットワークセキュリティサービスを提供する。MSP は依頼団体が自前でネットワークセキュリティを管理するより、より高度な専門性をもったサービスを同等のコストで提供できる。その結果、MSP は、企業が自ら全てのネットワークセキュリティの運営をすることに対する魅力的な代替手段を提供している。

ある団体が MSP の利用を選択した場合、通常当該団体と MSP との間で契約を締結することが必要となる。適切に起案されている場合、この契約は、契約当事者のうちでウィルス、ワーム及びソフトウェアの脆弱性に対してより防御能力を持つと思われる MSP に対して、ネットワークセキュリティ違反の危険を移転する機能を果たすことができる。

MSP サービス契約に関し、免責条項が広範に用いられなければ、このリスク移転戦略は広く利用されよう。しかしながら、セキュリティ違反に起因する顧客のシステムへの損害に対して MSP の責任を広範に制限する規定を含まない MSP のセキュリティサービス外注契約はまれである。その結果、現実的な契約戦略であるはずのものが、結局その牧歌的な約束を実現することに失敗したといえる。しかしながら、MSP は、保険がなければ契約で通常排除されるところの付随的損害及び結果損害に関し、一定の額まで、求償を認める保険が背後に付されている保証(warranty)プランを提供する可能性がある。MSP はこれらの損害に関し、顧客の損害を賠償した上で、保険会社に対して求償することができる。このようなプログラムの有効性は、保証がカバーする範囲及び損害を被った顧客に求償を認めることができる額の範囲如何といえる。

3．　ウィルス、ワーム及びハッカーの攻撃から生じたシステムの損害に対する保険

保険契約は、要するに損害を負担するにより適した立場にいる保険会社に一定の危険を移転する契約である。ウィルス、ワームまたはハッカー攻撃の損害を分散するために保険契約を締結することは、一見現実的な解決策に思われる。しかしながら、伝統的な保険契約は有体物の損害のみを対象としてきた。ごく限られた例外を除き、コンピュータデータのような無体財産に対する損害は、保険の対象とはならない。刑事犯罪を対象とする保険契約も通常は有体物の窃取等に対象が限定されており、その結果、ハッカーのように刑事犯罪としてのデータの窃取または破壊は伝統的な犯罪保険では保険対象に含まれない可能性が高い。更に、犯罪保険は、しばしば保険対象たる「犯罪者」を、会社を辞める従業員がデータを盗んだ場合や、従業員が第三者に不正取得させる場合に限定している。

物損保険及び事業障害保険における制約は、一般にこれらの保険が契約に規定されている危険のみを対象としていることである。その結果、火事、台風その他の明示された危険から損害が発生したのでなければ、物損または事業障害保険は明示されていない危険の結果としてのサイバー責任には適用されない可能性が高い。事態を更に複雑にしているのは、事業障害保険は事業全体に対する完全な障害が発生しない限り適用されないことがしばしばであることである。ウェブが一時間クラッシュすれば事業に不具合は生じるであろうが、このような事態が事業障害保険でカバーされることはまれである。

伝統的な保険契約では今日のテクノロジー主導の環境がカバーできないことは、今日のビジネスのリスクを特に対象とする保険の開発へと導いている。AIG, Chubb, Lloyd's of London, Zurich, Ace, Allianz その他の多国籍企業が提供するサイバー責任保険は、ネットワークまたはコンピュータセキュリティシステムをコンピュータ攻撃から守るができなかったことに関する被保険者のリスクを対象とする試みである。これには、被保険者のコンピュータへの無権限のアクセスまたは利用、コンピュータウィルスの他者への送信及び顧客情報の不適切な取得、破棄または第三者への開示が含まれる。ネットワークセキュリティを対象とする保険が主として対象としているのは、被保険者のシステムの無権限アクセスまたは利用に起因する損害である。

第三者によるネットワークセキュリティに関する法的主張は、しばしば不十分なネットワークセキュリティの結果生じるものであり、これらの保険の対象たる責任は、これらの法的主張に対応するものである。かかる保険は、サービスの拒絶または被保険者のシステムに由来するウィルスによる損害に関して第三者から訴えられた場合に、被保険者に提供される。またかかる保険は、

被保険者のシステムがサービス拒絶攻撃またはウィルス送信の道具として第三者に利用された場合にも被保険者に適用される。その他かかる保険の対象たる第三者の法的主張には、個人情報または秘密情報の開示に由来するもの及びテクノロジーサービスの規定に関連するミスや不作為に由来するものも含まれる。

事業障害保険の対象範囲も伝統的な保険よりはるかに広範である。殆どのサイバー責任保険における対象たる事業障害は、システムへの攻撃により被保険者がオンライン取引の収益を逸するという直接的な事業障害のみならず、攻撃または付随的事業の不全により被保険者が事業取引を行えないことに伴う付随的な事業障害の場合を含む。更に、保険対象たる事業障害は、一定期間の事業障害で全体的かつ完全な障害には至らない場合にも適用されうる。

4．スラマー仮設事例における契約責任の主張

第 1 章におけるスラマー仮設事例において、原告にワームを送信しないように注意し、攻撃を防御し、または原告のシステムの脆弱性を除去する契約上の義務があるいずれの上記当事者に対しても、原告は法的主張ができると思われる。直接損害は、契約に基づき原告が受ける製品やサービスの契約上の価値から原告が実際に受けた価値を引いた差額である。契約違反に基づく価値の減少を測定するのは容易ではなく、必然的に購入価格またはライセンス料の一部となる。事案によっては、関連する契約により払い戻しや取替えを唯一の救済方法と指定することがあるが、いずれにせよ損害は製品の価格を超えることはない。それゆえ、付随的損害や結果損害が契約により効果的に排除されていれば、潜在的損害は極めて限定的となってしまう可能性がある。本件では、契約責任の主張は、契約価格が高額であるか、または原告がクラスアクションを提起できる条件を満たしたクラスに属する場合に限り、経済的合理性があるといえるかもしれない。

直接の契約関係(privity)が必要なことは、契約責任の主張をする上で、とりわけ典型的なネットワークセキュリティ違反事案で、大きな制約となっている。スラマー仮設事例では、SQL スラマーワームによりコンピュータシステムに損害を被った原告は、原告にワームを拡散したことに責任があるシステムを運営していた当事者に対し訴訟を提起している。仮設事例では、ワームの拡散以外原告と被告の直接の関係がないことが前提となっている。原被告間には、契約関係がないということになっている。その結果、契約違反の主張に必要な直接の契約関係を欠いている。従って、原被告間でスラマーワームのような害意あるソフトウェアを拡散することを防止するための管理を被告が行うといった類の合意がなされていない限り、または原告が被告と第三者間の契約の意図された受益者でない限り、スラマー仮設事例で原告が契約違反の主張をしても認められないであろう。

D.　ガイドライン

米国では、業界全体にかかるネットワーク協会のルールもまた、情報セキュリティの制約を課すことがある。これらのルールは、契約によりかかるルールに従って業務を行うことに合意している場合には、拘束力がある。このような場合として下記の例がある。

- 全米自動手形決済所協会(The National Automated Clearing House Association)　(以下「NACHA」という。)の運営規則は、自動手形決済を行う金融機関及び商人に対しセキュリティの制約を課している。
- クレジットカード協会及びクレジットカード会社は、商人や金融機関にセキュリティに関する制約を課している。
- 保護された B2B 取引のための認証手続きが、Identrus LLC 社によって、金融機関の協会のために設けられている。

これらのガイドラインに加え、様々な団体が情報セキュリティに関するベスト・プラクティス及びセキュリティ監査の方法を開発し、情報セキュリティを改善しようとする組織にガイダンスを提供している。これらに関し、下記の例がある。

- 最も広く引用されまた利用されている情報セキュリティに関するベスト・プラクティスである ISO スタンダード 17799。
- 通常の分類に従った評価スキームとして ISO/IEC 15408-1 を参照。
- アメリカ公認会計士学校の監査方法である「トラスト・サービス」 http://www.aicpa.org/assurance/trustservices/index.asp
- CERT という組織が公表しているシステムとネットワークセキュリティプラクティスの一般的ガイド。http://www.cert.org/homeusers/cert guide.html
- SANS インスティトゥートもまた情報セキュリティに関するガイダンスを提供している。インターネット・セキュリティ・センターと共同で開発したベスト・プラクティスは、http://www.sans.org/score/で見ることが出来る。
- ナショナル・インスティトゥート・オブ・スタンダード・アンド・テクノロジーもまた、特に連邦政府を対象としたベストプラクティスを提供している。
- デジタル・リスク・アンダーライティング・アンド・マネジメント協会（DRUMS）は、保険業界を対象とするスタンダードを開発に取り組んでいるところである (www.drumsnet.org 参照)。

第 3 章　2003 年 4 月 29 日付け質問に対する回答

3.1　定義

3.1.1　脆弱性を議論するにあたって、「ソフトウエア」の定義が法にありますか。

回答：情報セキュリティに対する脅威に適用される制定法、行政規制その他の法律で、「ソフトウェア」につき特に定義してあるものはないと理解している。しかしながら、ソフトウェアは情報セキュリティのコンテクストの範囲外で定義がなされる法令がある。例えばコンピュータソフトウェアレンタル修正法(17 U.S.C. §101)等で定義されている。

3.1.2　「セキュリティホール」「脆弱性」「不具合」について法令等で定義をしていますか。

回答：情報セキュリティのコンテクストでこれらの概念を特に定義してある制定法、行政規制その他の法律はないと理解している。

3.1.3　「セキュリティ・ホール」という用語が法令等で使用されていませんか。

回答：情報セキュリティのコンテクストでこれらの概念を特に定義してある制定法、行政規制その他の法律はないと理解している。

3.2. 責任(Liabilities)

3.2.1　一般的フレームワーク (General frame work)

情報セキュリティ脆弱性もしくは不具合からの責任について、定義や責任が定められていますか。
もし、必要であれば、請求原因を不法行為、制定法、契約法に分けることもかまいません。
民事上の責任について詳細に記述してください。ただし、脆弱性の濫用に対しての刑事的責任および行政的手法についても概観をしてください。

以下の責任についての論点を考慮にいれて報告ください。

(a)　ソフトウエアまたはハードウエアに欠陥があった製造者,開発者の責任
(b)　「下流責任」(情報セキュリティ侵害攻撃を停止するのに失敗した最初の被害者の責任、すなわち、そのシステムが他者のシステムを攻撃するのに利用された責任-公開されたパッチを宛てるのを怠った責任や公知の脆弱性に対応するのを怠った責任)
(c)　システムにおける脆弱性を発見するために効果的な監査を怠った際の責任

回答：情報セキュリティの脆弱性または欠陥に関し、不法行為法、制定法及び契約法の範疇で、責任を定義し確立している法律は、上記のとおりである。
(a) 製造者及び開発者の責任は契約のセクション及び不法行為法のうちの製造物責任のセクションで論じられている。
(b) 下流責任のシナリオは、不法行為法の部分で議論されている。
(c) 最後に、システムにおける脆弱性を発見するために効果的な監査を怠った際の責任は、原告が効果的な監査を受けるために被告と契約していた場合には契約責任に帰結し、また原告と被告の間に契約関係が存在しない場合には不法行為責任に帰結しうる。

3.2.2：セキュリティ法的責任の要素(Elements of security legal liability)

情報セキュリティ、機密性、正確性、可用性と法的責任には、どのような関係がありますか。

回答：HIPAA 法を実効あらしめる規制は、HIPAA 法でカバーされているヘルスケア団体に対し、予見可能なセキュリティに対する脅威のコンテクストにおいて、患者の記録の秘密性、完全性及び入手可能性を保証することを義務付けている。HIPAA 法違反は、罰金または懲役という刑事罰の対象となりうる。

3.2.3 主体的側面(Subjective aspect)

情報セキュリティに対する侵害があった場合に、被害者から責任を追求され得る当事者についてあげて下さい。

具体的に以下の例について記述して下さい。

- ハッカー(脆弱性に対して攻撃するソフトウエアを開発し、意識的に配布するもの)
- 脆弱性の存在するハードウエアまたはソフトウエアの製造業者または開発者
- コンサルタント、システムインテグレーター、配布者、販売業者、その他脆弱性有る技術を推奨したベンダー
- セキュリティの評価やセキュリティ脆弱性の回避を委任されたコンサルタント
- 脆弱性を発見する監査人
- 攻撃を抑止するように依頼していたセキュリティ・プロバイダー
- アプリケーションを最新に、パッチを宛ててもらうことにしているアプリケーション・サービスプロバイダー
- システムをアウトソースしている場合のホスティング会社
- 攻撃を許容し、または、停止し得なかった ISP
- 脆弱性を発見していながら、それを被害者、ベンダーまたは公に報告しなかった者

回答：本質問に記載されている全ての個人は、個別具体的な事案に応じて、不法行為、制定法、及び/または契約法理に基づき責任を負う可能性がある。その他の責任主体となる可能性がある当事者としては、ハッキングや情報セキュリティに対する攻撃がなされる前に脆弱性に関し公開し、かかる公開行為が不正者の行為を助長したことを原告が証明できた場合の、かかる公開当事者たる組織がありうる。

3.2.4 脆弱性の場所

以下のような脆弱性の発生個所によって、責任を問われる人が異なりますか？
- クライアント側
- サーバ側
- ネットワーク機器部分
- など

回答：法律は責任の所在を決定するにあたり脆弱性の発生場所による区別を一般的にはしていないと理解している。しかしながら、契約により発生場所に重要性を付加することはありうる。例えば、ASP の顧客が、ASP が管理するサーバーの脆弱性に起因した損害を被った場合、サーバー側の責任として ASP の責任が契約上規定されていれば、顧客は脆弱性の発生場所を理由に ASP の契約責任を問うことができると思われる。なお本報告

書の回答の範囲外ではあるが、脆弱性の場所は、準拠法の決定に影響しうる。

以下のようなソフトウエアの提供形態によって、責任の違いを区別しているかを解説してください。
- パッケージ品ソフトウエア（市販品）
- 個別開発品ソフトウエア
  - 外注（成果物検収 Deliverable）
  - 委託（工数検収 Labor hour）
- サービス提供に利用しているソフトウエア
- など

回答：ソフトウェアのタイプの違いが不法行為や制定法に基づく法的主張に影響を及ぼすことはないと考える。しかしながら、契約に基づく主張に関しては、物品の販売契約、無体財産(例えば情報)取引契約、またはサービス契約であるかが黙示の保証(implied warranty)の成否に影響すると考えられる。かかる差異は、ソフトウェア開発者及びソフトウェア受注者間で黙示の保証に関する権利放棄(disclaimer)がなされる場合には重要な問題とはならない。実際には、流通しているエンドユーザー向販売用ソフトウェアは殆ど全てこのような権利放棄を含んでいる。更に、特に開発されたソフトウェアに関するライセンス契約も、大抵、このような権利放棄を伴っている。かかる権利放棄が有効に責任を制限できるか否かは、個別具体的な問題であり、本件のような一般的な質問に対する回答という形では結論付けられない。

3.2.5 注意義務-標準(Duty of care-standard)

3.2.5.1 一般(general)

法によって情報セキュリティの基準が定義されていますか。
脆弱性の改善義務についての基準を法令等で設けているか？
法令等以外の情報も知っていれば教えてください。

回答：ある当事者にウェブサイト上のセキュリティホールを修復する義務があるか否かは、上記過失責任のセクションで論じたとおりである。不法行為法のもとでは、当事者は一般に他者に対しアシストをする義務はなく、従って他者運営のウェブサイトや他者作成のソフトウェアに存在する脆弱性を修復することに関し他者を助ける一般的義務があるとは考えがたい。しかしながら、契約法上は、製造者から提供されたソフトウェアの脆弱性は、契約違反とみなされる可能性があることは上記のとおりである。また、脆 弱性につき警告することを怠った場合には不法行為法上の厳格責任が発生する可能性がある。保険会社は、一般に、サイバー責任保険を提供する条件として、最高の情報セキュリティを実践するよう働きかける。不法行為法、制定法及び契約法のセクションで論じたように、米国法には情報セキュリティ保護のための注意義務の基準につき定義しているものがある。契約の場合、契約履行に際してどのような注意義務を課するかを当事者が自由に決定し定義できる。

3.2.5.2. 管理者の義務 (Duties of administrators)

システム管理者が、不具合を修正するためになすパッチやソフトウエアを使用することを怠った場合、責任があるか。

システム管理者がセキュリティ情報を収集するのを怠ったとき、責任があるか。

回答：システム管理者（またはその従業員）は、職務を適切に遂行しなかった場合には責任を負う可能性がある。彼らの行為が、彼らと契約関係にない下流の犠牲者に損害を生ぜしめた場合には、状況によってはこれらの下流の犠牲者に対し過失責任を負う。適切なセキュリティのプロセスを取ることを怠った当事者と契約関係にある者が損害を被った場合には、当該契約にパッチを施したりソフトウェアをインストールして損害の拡大を防ぐ義務が規定されていることがあり、その場合には、契約に規定したかかる義務に違反している限り契約不履行責任を構成しうる。

3.2.5.3 インシデントにおけるシステム管理者の義務（Duties of system administrators in case of incidents）

インシデントに対応する際、システム管理者は、不十分な対応しかできなかった場合、または、対応がおくれた場合、責任を負うか。
損害を回避する責任を負う当事者が他にいますか。

回答：下流の犠牲者が、上流の当事者が十分に情報セキュリティ違反に対応しなかったり、対応が遅れたために損害を被った場合、下流の犠牲者は（契約関係がない場合）上流の当事者の対応に関する注意義務違反を理由に法的責任を追及しうる。かかる主張が認容されるか否かは個別具体的な事案如何である。管理セキュリティプロバイダー(MSP)のように、対応に関し他者を助けることが契約上規定されている場合には、かかる当事者が契約上のかかる義務を履行しない限り、契約不履行の責任を負う可能性がある。

3.2.5.4. セキュリティ・ポリシー(Security policies[2])

3.2.5.4.1 **注意義務の標準として、法はセキュリティポリシーを必要としていますか。**

回答：不法行為法において、セキュリティポリシーの欠如が当事者の損害の重要な要因であれば、セキュリティポリシーの欠如自体が過失責任を構成しうる。HIPAA 法や GLBA 法に基づく制定法及び行政規制は、実際にセキュリティポリシーの文書化を要求している。もちろん契約上の取り決めによりかかるポリシーを義務付けることもできる。

3.2.5.4.2 **保険会社や産業界の事業者協会で、ガイドラインを標準としていることはないですか。**

回答：第 2 章 D 参照。

3.2.5.4.3 **セキュリティポリシーの実際の運用が責任に対する抗弁になりますか。**
セキュリティポリシーの実際の運用が連邦ガイドラインのようにコンプライアンスの観点から考えられていますか。

回答：セキュリティポリシーの実際の運用が責任に対するセーフハーバーになる旨規定している法律はないと理解している。但し、ポリシーを遵守したことは、合理的注意を払ったことの証拠となり、過失責任を否定する根拠となりうる。対照的に、当事者は契約においてセキュリティポリシーを遵守する旨約束し保証するが、それ以上の義務に関しては合意していないことがある。このような場合、セキュリティポリシーで要求されていない手順を踏まなかったからといって、契約不履行責任を負う

[2] In this context," security policies" have broad meaning and include "Implementations, Planning and Audit"cycle.

ことはない。

3.2.5.4.4　セキュリティ上の脆弱性が、セキュリティの監査および評価をしていながら、それを探知できなかった場合、その監査および評価をしていた事実は、抗弁となりえますか。

回答：その監査および評価をしていた事実が責任に対するセーフハーバーになる法律はないと理解している。但し、契約により当事者は、かかる監査や評価が契約に従って履行された場合には、たとえ監査や評価では突き止められない脆弱性が後に発覚しても、免責されまたは責任が限定される旨取り決めることができる。

3.2.6 その他（Miscellaneous）

3.2.6.1　セキュリティ・インシデントの実体を明らかにするのに有効だと考えられる法的システムはありますか

回答：下記回答 3.3.4 参照。

3.2.6.2　「内部告発者保護」や「司法取引」の法制度を有していますか。

回答：米国の連邦法及び州法レベルでは内部告発者保護制度及び司法取引があるが、情報セキュリティに特に適用される法律はないと理解している。連邦科刑ガイドライン及びCFAA 法等の制定法は、サイバー犯罪に関する制定法違反に対し相当の刑罰を科する旨規定しており、被告人が司法取引に従い罪状を認めた場合に適用される。

3.2.6.3 「内部告発者保護」や「司法取引」の法制度が、セキュリティ・インシデントの実体を明らかにするのに有効と考えられるのではないかという議論はありませんか。

回答：前記 3.2.6.2 参照。

3.3 責任有る開示の問題（Responsible disclosure issue）

3.3.1 脆弱性に気がついたとき、気がついた人間は、会社や公的機関に報告すべき義務がありますか

回答：製造者により消費者に対し、自己の製品の知れたる脆弱性を開示することに関しては、製造者が消費者に対しかかる開示を怠った場合には、CFAA 法に基づき責任を負う可能性がある。また、製造者または開発者は、かかる開示が契約上要求される場合には、かかる開示義務を負う。またかかる開示義務は不法行為法の厳格責任として課される可能性がある。製造者や開発者の注意義務には、過失責任のコンテクストにおいて警告する義務が含まれる可能性がある。

セキュリティの脆弱性に関して消費者が報告する一般的義務があるとは認識していない。但し、契約で消費者にかかる義務を課すことは可能である。

然るべき行政機関等への報告義務に関しては、上記第 2 章 B.3 参照。

3.3.2 報告された会社などは、これに対して対応すべき義務はありますか。また、対応をなしうる体制をとっておく義務があると解されていますか。

回答：かかる体制をとっておく一般的法的義務があるとは認識していない。

3.3.3 産業界や政府の機関が、脆弱性がわかった際に、それに対して責任有る開示となるようなガイドラインを準備していますか。もし、準備している際は、その内容をお教えください。

回答：インターネットにおける「責任ある開示手続き」に関する草案がインターネット・エンジニアリング・タスクフォースに提出されている。プロポーザルがなされた時点で報告可能となる。

3.3.4 脆弱性の報告について、その内容を分析する専門的な委員などの制度が提案されていませんか。もし、議論されているのであれば、その内容をお教えください。

回答：下記追加回答２参照。

3.4　SQL Slammer の事件をきっかけに何か動きなどがありましたか？

回答：特に認識していない。

3.5　「ソフトウエアの脆弱性に対応するガイドライン」の観点でご意見があれば教えてください。.

<u>追加回答</u>

1. ナショナル・インフラストラクチャー・アドヴァイザリー・カウンシルという団体があり、政府が資金援助を行っている。2003 年 3 月 1 日、米国大統領は国土安全省（Department of Homeland Security）("DHS") に対し、資金援助をすべく行政命令を行った (http://www.dhs.gov/dhspublic/display?theme=43&content=817 参照)。従って、今後は DHS の予算の中にセキュリティに関するカウンシルの補助金を見出すことが出来る。

   また、私的団体である手形交換所は、脆弱性ある開示に関し、政府から補助金を受領しているものがあるか否かに関しては、このような団体があることを認識していない。

2. DHS の一機関である FedCIRC に関しては、特にその下部機関であるパッチ認証配布センター (the Patch Authentication and Dissemination Center)が特に注目される。同センターは、ウェブ上のサービスとして、会員や連邦政府機関に下記のようなサービスを提供している。

   - 「攻撃の脅威や脆弱性に関する適時の通知」
   - 「認証されたパッチのダウンロードの保証」
   - 「テクニカル・ヘルプデスク・サポート」

   プライベートセクターに関しては、DHS は CERT Coordination Center と協力して、PADC が連邦政府機関に提供するものと概要において同等のサービスを提供するよう計画している。但し、いずれのプログラムもまだ大部分において計画段階に過ぎないことに留意する必要がある。

3. よりよいセキュリティを実現するための業界の私的取り組みや声明は、執行力を伴う法律ではなく、遵守しなくとも責任が発生するわけではない。そのため、このような声明は、(例えばソフトウェア製造業者のような)セキュリテイレベルの低い状態を変えさせるためには、殆ど役に立たない考える行政担当者もいる。他方、行政を指示する者の中には、過度の規制や責任は有害無益であると主張する者もいる。

『セキュリティホールに関する法律の諸外国調査』報告書

付録　Ｂ－２

カナダ　報告書日本語訳

（余白）

カナダにおける情報セキュリティ責任

日本国経済産業省に対する報告書

２００３年6月

監修者：ジョン・D・グレゴリー（カナダ、オンタリオ州トロント）

カナダにおける情報セキュリティ責任
序論
ジョン・D・グレゴリー

インターネットを通じてのＳＱＬスラマー・ウイルスの最近の拡散は、多くの国にかなりの損害を生じた。日本では、経済産業省が、将来の同様の攻撃を如何に避けるか検討しているところである。同省の調査部門の一つは、ウイルスの拡散の法的要素であった。可能な責任項目は何か、および、どのように人々の行為が法的責任の予見により影響されるのか？

この文脈において、経済産業省は、カナダを含む数カ国における情報セキュリティ侵害の法的意味の研究を委託した。

カナダにおいて民事責任法は、州法上の責任である。刑事法は連邦法上の責任であり、カナダ刑事法典は全土に適用される。しかしながら、情報セキュリティ侵害の法的意味の多くは民事に関する事項であり､州法に関わる｡カナダ法の全体理解の確保のため､問題点に関する２つの検討が求められ､それらはこの文書に添付されている。

２つの検討が必要であった理由は、カナダが二つの法制度をとっているからである。１０州のうちの９州は英国のコモン・ローに基づく英米法制度をとっている。これは、カナダが連合王国のかつての植民地であることに由来するが、当然、１８６７年の国家としてのカナダ創設以来、独自の裁判所および立法府により発展してきている。

もう一つの州である、ケベックは、フランス民法典の諸原則にもともと基礎を置く、大陸法制度をとっている。ただし、現在のケベック民法典は、１９９４年にようやく施行された。日本は大陸法の伝統を有しているので、諸問題に対するケベックのアプローチはとりわけ有益であると考えられる。

英米法に関する回答は、トロント大学法学部法政策革新センターの後援で準備された。大陸法に関する回答は、モントリオール大学法学部公法研究センターを通じて準備された。

このような場合にありがちなことだが、二つの制度のもと認識された結果が、推論が違う経路を辿りながらも、しばしば相互に類似していることに気付く。ケベックを含む、カナダの制度はアメリカ合衆国およびヨーロッパに由来する知的なかなりの影響にさらされている。それらの影響は、両検討に明らかである。加えて、カナダの英米法裁判所は、主たるコモンウェルスの英米法域からの判例と同様に、ある法領域に関してはアメリカの判例を興味深く読んでいる。

両検討とも、もっぱらその執筆者に関わるもので、センターまたは大学には関わりない。両検討とも、依頼者に対する法的助言ではなく、執筆者に可能な限り正確を期した分析であり、経済産業省が提起した質問に対して､カナダの英米法または大陸法制度の法的諸原則がどのように適用されるかに関する、確定的というよりはむしろ一般的な推論である。

これらの文書が、世界のすべての地域に影響する、コンピュータ・システムにおける脆弱性への対応の検討に際して、経済産業省への助力となることを希望する。

モントリオール大学
法学部
公法研究センター

経済産業省による委託
「情報セキュリティ責任質問事項」への回答

２００３年6月6日

本分析は、「公法研究センター」サイバースペース法チームによりなされたものである。

プロジェクト・コーディネイター：カリム・ベニックェレフ教授
意見起草：ニコラス・ヴェルミース

公法研究センターは、その研究者により提出された意見を保証するものでなく、また非難するものでもない。これらの意見はもっぱら執筆者に属するとみなされるものとする。

以下の法的意見は、日本国経済産業省２００３年５月２９日付け委託「情報セキュリティ責任質問事項」（経産省質問事項）に応えて起草されたものであり、示された法的争点に関するわれわれの理解、およびケベック州法にもとづいて明らかなことに厳格に基づいている。

大陸法の州であり、上述質問事項に応えるケベック州は、幾分問題があることが明らかとなった。その理由は、ケベック州は、われわれの想起する法制度と考え合わせてこられたように思われないからである。ケベック州の立法は、大多数の法状況に向ける目的で、広義に書かれており、かつ個別の争点を解決するようには滅多に作られていない。例えば、ケベック州における民事責任は、状況ごとに異なる不法行為類型からなる英米法制度とは異なり、その者に（四囲の状況、慣行または法に従って）[i] 課せられている行為規範を遵守しないことによって他者に侵害を生じた者には過誤があり、被害当事者に完全に補償しなければならないという一般原則によって律せられている。ケベック州民法典第１４５７ないし１４８１条に確立されたこの一般原則は、責任がコンピュータ・セキュリティ問題、瑕疵担保、または殴り合いのいずれに由来するかによらず、すべての責任問題に適用される。

また加えて置かなければならないことは、ケベック州の裁判所は、経産省質問事項に示されたような諸問題に既に直面しなければならない事である。従って、以下の分析は、長年にわたりケベック州の判例法及び法学の教科書により確立されてきた一般的法原則に基づく十分に知られた推論からなる。

コンピュータ・システムの脆弱性に帰されるコンピュータ・ウイルスの移転を理由とする法的責任

上述のように、ケベック州の裁判所は、コンピュータ・ウイルス責任に関わる事件に既に直面しなければならなくなっており、この問題を取り扱っている著者はほとんどいない。[ii] 裁判所に提起された場合に、裁判所がこの争点をどのように処理するか予見することは依然不可能であるけれども、ケベック州および他の法域における類似の責任問題に焦点を合わせることによって、ケベック州法に基づく基本的責任原則に照らして、ウイルス責任の問題をどのように取り扱うべきかに関する一般的見地を引き出すことは可能である。

ケベック州民法典第１４５７条は以下の通り。

何人も、他者に侵害を生じないよう、四囲の状況、慣行または法に従って、課せられている行為規範を遵守する義務を負う。

分別を有し、かつ、この義務に違反する場合には、そのような過誤により他者に対して生じたいかなる損害を理由とする責任があり、侵害が身体的、道義的または物理的のいずれであろうと、その侵害の補償をなす責任がある。

また、一定の場合には、保護下にある他者の行為または過誤により、または保護下にある物のしわざにより他者に生じた侵害を補償する責任がある。

本条の分析において、裁判所は、責任を立証するためには、過誤、損害、および二者間の因果関係を立証しなければならないことを確立している。[iii]

過誤

過誤は二つの異なる方法で推断されうる。最も簡単かつ最も平凡なものは、被告は法に違背する行為を遂行したことを立証することによる。[iv] 第二は、その適用がより複雑であるが、被告は、他者に害を生じない一般的義務に違反したか否かを決定することによる。[v] これは、合理的、分別のある、注意深い個人であれば、非難されている行為を避けたはずであったか否かを検証することによってなされる。[vi] セキュリティの不備の存在を禁じている法律はないので、他者を害さない一般的義務の範囲で、脆弱なセキュリティ・システムを有することが過誤に当たる行為と考えられるか否かを認定できる。このことは、第一の状況を生ずる。すなわち、「この点で、不法行為訴訟において依拠できる行為標準はない。実際、「合理的なコンピュータ・プログラマー」であれば、当該状況下で何をなしたかについて、相当量の議論がある。」[vii]

裁判所により確立されていることは、過誤は故意であっても、過失に由来するものでもよく、他者

に侵害を生じないためのすべての通常要請される予防措置をとらないものと要約されうる。[viii] 従って、コンピュータ・ウイルスに関する文脈においては、自己のシステムを侵入から防止するためのすべての通常要請される予防措置をとらない当事者には過失があり、従って過誤があると主張され得よう。問題は残る、つまりコンピュータ・セキュリティの文脈においては、何が「通常要請される予防措置」と考えられるべきか？この問題を取り扱う一つの方法は、産業界では何が慣習かに目を向けることである。仮にシステム・管理者の９０％が技術Ａまたはそれより良いものを使用していれば、技術Ａの使用は通常要請される予防措置であると論じられる。しかし、カナダ最高裁判所が述べるところでは、産業界の標準に従っても、個人が責任なしと判示されることを保証しない、その理由は、そのような標準は産業界のために産業界が作り出したものにすぎないからである。[ix] しばしば、そのような標準に究極的には影響される人々（例えば消費者）はそのようには発言しない。したがって、何人かの著者が示唆していることは、コンピュータ・セキュリティの場合には、通常要請される予防措置はシステム・管理者が現に知り、または存在を知っているべきであるすべての合理的に入手可能な技術を使用することとすべきである。[x]「通常要請される予防措置」という表現が何を意味するかに関して、示唆されていることは[xi] 見込まれる損害（危険率を乗じた評価損害）[xii] より高価でないすべての技術は、合理的に入手可能と考えられるべきであることである。

損害

コンピュータ・システムの故障により生じた損害は、様々な形態をとりうる。最も著しいのはシステム及びデータの損失を「復旧」に伴うコストである。しかしながら、データの損失には幾分問題がある、というのはデータそのものが「物」でないからである。データは有形でない、そのことはアメリカの裁判官にデータの喪失は損害でないと考えさせた。その理由は、「物」すなわちデータが蓄積されているディスクはウイルス攻撃によっては滅多に無能力化されないからである。[xiii] 幸運にも、このような判断は最近の判例法ではもはや支持されていないが、[xiv] ケベック州の裁判官がこの問題を将来どのように取り扱うか依然注目されるべきである、というのも、われわれの裁判所ではまだ議論されなければならないからである。

因果関係

過誤は損害の直接の原因でなければならない、または損害は過誤の直接の結果でなければならない。[xv] それがケベック州法に基づく因果関係の定義である。多くの場合に、因果関係は明白である。すなわち、私があなたを撃ち、あなたが弾丸で死ぬ場合、私があなたを殺したのは明白である。しかし、二人の人がほとんど同時にあなたを撃ち、両射撃とも致命的な場合はどうだろう？あきらかに、一つの弾丸は何も損害を生じていない、なぜならそれが命中したときあなたは既に死んでいたのだから。このことは大陸法では、二人の狙撃者のうちの一人は侵害しておらず、かつ、どちらであるか証明が不可能であるから、どちらも責任なしと判示されるべきことを意味するかもしれない。同様な問題がコンピュータ・システムの脆弱性の場合にも存在する。あるシステムが、二つの異なるソースにより移転された同じウイルスの二つのコピーにより攻撃された場合、どちらに責任があるかどのように立証できるだろう？そのようなジレンマを解決するために、ケベック州の立法者は次の整理を提案した。

第１４８０条複数の者が侵害の結果をもたらす不法な行為に共同で参加し、またはそれぞれが侵害を起こしたかもしれない別々の過誤をなした場合、かつ、いずれの場合にも、どちらが実際に侵害を生じたかを決定することが不可能な場合、かれらはその保証に関して連帯責任を負う。

したがって、民法典のこの整理は、事実的因果関係、および二当事者に過誤があるが、一方だけが損害を発生させた場合の現在の蓋然的因果関係を、被害者が脇に押しやることを認めた。

＊＊＊

一般的基礎は以上の通りである。ここでわれわれは、回答を求められている質問事項を詳細に見ることができる。

脆弱性を議論するにあたって、「ソフトウエア」の定義が法にありますか。

「ソフトウエア」という用語はケベック州法下で定義されておらず、また脆弱性問題と責任に関するいかなる判決においても定義されていない。

「セキュリティホール」「脆弱性」「不具合」について法令等で定義をしていますか。
民法典第１４６９条が説明するところでは「物に安全性欠陥があるのは、あらゆる状況を勘案して、人が通常期待する権利を有する安全性を当該物が提供していない場合であり、特に当該物のデザインまたは製品の欠陥、当該物の劣悪な保存または提示、もしくは当該物が有するリスクおよび危険性、または安全防止措置に関する十分な表示の欠如がその理由である場合。」ケベック州は大陸法に属する州であり、そのような広範な定義は、コンピュータ・セキュリティ問題が法廷に持ち込まれる場合には、そのような問題にも適用されることは疑いない。

「セキュリティ・ホール」という用語が法令等で使用されていませんか。
「セキュリティ・ホール」という表現は、ケベック州法全集には存在しない。

3.2. 責任(Liabilities)

3.2.1 一般的フレームワーク (General frame work)

情報セキュリティ脆弱性もしくは不具合からの責任について、定義や責任が定められていますか。
もし、必要であれば、請求原因を不法行為、制定法、契約法に分けることもかまいません。
民事上の責任について詳細に記述してください。ただし、脆弱性の濫用に対しての刑事的責任および行政的手法についても概観をしてください。

以下の責任についての論点を考慮にいれて報告ください。

(a) ソフトウエアまたはハードウエアに欠陥があった製造者,開発者の責任
(b) 「下流責任」(情報セキュリティ侵害攻撃を停止するのに失敗した最初の被害者の責任、すなわち、そのシステムが他者のシステムを攻撃するのに利用された責任-公開されたパッチを宛てるのを怠った責任や公知の脆弱性に対応するのを怠った責任)
(c) システムにおける脆弱性を発見するために効果的な監査を怠った際の責任

上述のように、ケベック州は大陸法の州であり、われわれの州法[xvi] は、すべての考えられる状況をカバーするように考えられる最広義に立法されることを意味する。こういえば、ほとんどの責任問題は、それらがコンピュータ・セキュリティに関するか、遊歩道で泥水に滑ったことに関するかによらず、民法典第５編第３章「民事責任」の範囲である。同章の一般規定は次のように述べる。すなわち、「何人も、他者に侵害を生じないよう、四囲の状況、慣行または法に従って、課せられている行為規範を遵守する義務を負う。分別を有し、かつ、この義務に違反する場合には、そのような過誤により他者に対して生じたいかなる損害を理由とする責任があり、侵害が身体的、道義的または物理的のいずれであろうと、その侵害の補償をなす責任がある。」[xvii]
製造事業者または開発業者の責任に関して、民法典第１４７３条は次のように追加する。すなわち、「動産の製造事業者、頒布者、または供給者は、同動産に安全性の欠陥が生じた侵害を理由とする補償に対して、同人が、被害者が当該欠陥を知り、または知りえたこと、または当該侵害を予見しえたことを証明する場合には、責任を負わない。また、同人が当該動産を製造、頒布、または供給した時点の知見状態に従えば、欠陥の存在は知り得なかったこと、および同人が当該欠陥を知るに至った時に情報を提供する同人の義務を怠っていないことを同人が立証する場合には、同人は補償責任を負わない。」逆に、これが意味するのは、コンピュータ・ソフトウエアの製造業者または開発業者が、そのソフトウエア、またはパッチの欠陥を知っており、かつ依頼者に対して当該欠陥について警告しない場合には、過誤あるソフトウエアにつながるセキュリティ侵害に対する「過誤の深刻さに比例して」

[xviii] 責任を負うと判示されうることである。「過誤の深刻さに比例して」という語句は重要である。その理由は、責任は「侵害が複数の者により生じた」[xix] 場合には連帯されるという考えに立ち返るからであり、ウイルス攻撃を検討する事件であることは疑いない。

そのような認識はまた下流責任原則の適用可能性ある事件を生み出す。ケベック州法に基づけば、英米法域と同様に他の多くの大陸法と同じく、責任を立証するためには、３要件を充足しなければならない。すなわち、過誤、侵害、および二者間の因果関係である。上述の仮説的事例に沿っていけば、侵害の立証は十分に容易であろう。[xx] 過誤と第三者の関与の間の因果関係も、システムへの攻撃を遡ることが出来れば、容易に認識可能である。したがって、唯一残る問題は、過誤についてである。筆者の信ずるところでは、公にされたパッチの適用をしそこね、よく知られた脆弱性を取り扱わない者には過失がある。その理由は、同人は彼の行動が他者に侵害を生じないように、[xxi] すべての通常要請される予防措置を講じていないからである。過失は過誤を意味する一つの方法であり、[xxii] したがって、民事責任を立証するすべての必要要件を充足しているので、下流責任はケベック法に基づいて可能な手段であると主張することが出来る。

システム内の脆弱性発見のための効果的な安全性評価を怠ったことに関しては、そのような懈怠は、合理的かつ勤勉な個人[xxiii] であればそのような職務を遂行していたはずであると立証できる場合にのみ、過失であると考えられ、従って責任を含む。

刑事責任に関する限りでは、カナダ刑事法典(R.S.C.1985, c.C-46)第３４２．１条は、以下のように述べる。すなわち、

第３４２．１条第１項　何人も、詐欺的かつ権利の外観なしに、
(a)直接間接にコンピュータ・サービスを受け、
(b)電磁的、音響的、機械的またはその他のデバイスの方法で、コンピュータ・システムのいかなる機能に、直接間接に、干渉し、または干渉される原因となり、
(c)(a)または(b)に基づく犯罪、もしくはデータまたはコンピュータ・システムに関して第４３０条に基づく犯罪を遂行する目的で、コンピュータ・システムを、直接間接に、使用し、または使用される原因となり、または、
(d)(a)(b)または(c)に基づく犯罪を人が遂行することを可能にするコンピュータ・パスワードを使用、保持、取引、または他者がアクセスする事を許す、
場合には、正式起訴犯罪で有罪とし、１０年未満の拘禁刑に処するか、または略式判決で科刑しうる犯罪で有罪とする。

本条が意味するのは、法的正当性のないすべてのハッキングは、脆弱性に関して区別せず、違法である。こういえば、論理的には、誰しも脆弱なシステムにしか侵入できないといえるかもしれない。しかし、明らかなことはシステムへの侵入の容易か困難かは、ハッカーの刑事責任には影響しない。ただし、侵入されたシステムの所有者の民事責任は影響を受けるかもしれない。

3.2.2：セキュリティ法的責任の要素(Elements of security legal liability)

情報セキュリティ、機密性、正確性、可用性と法的責任には、どのような関係がありますか。

この関係を取り扱うためにケベックの法律家に与えられている道具は最近の「情報技術への法的枠組みを確立するための法律」(R.S.C.2001,c.C-1.1)[xxiv] に由来する。同法第２２、２６、３６および３７条は、下記に掲げるが、民法典第１４５７ないし１４８１条（これらは責任を規定する）を、情報セキュリティ、秘匿性、完全性、または可用性、及び法的責任に関する限りで、補完する。

第２２条　接続業者として行為し、コミュニケーション・ネットワーク上で文書保管サービスを提供するサービス・プロバイダーは、サービス利用者により、またはその注文により保管された文書を使用するサービス利用者による関係諸活動に責任を負わない。

ただし、特に、当該文書が不正な活動に利用されている事に気付き、またはそのような使用が明白となる状況に気付きながら、サービス・プロバイダーが、当該文書へのアクセスをブロックするか、または活動の遂行を妨げる適切な行動をとらない場合には、サービス・プロバイダーが責任を負うこともありうる。

同様に、索引、ハイパーリンク、ディレクトリー、または検索ツールなどの、技術に基礎を置く文書参照サービスを提供する接続業者は、そのようなサービスの利用者による関係諸活動に責任を負わない。但し、特に、当該文書が不正な活動に利用されている事に気付きながら、そのような活動に関係しているとサービス・プロバイダーが知る者に対するサービス提供を停止する適切な行動をとらない場合には、サービス・プロバイダーが責任を負うこともありうる。

第２６条　技術に基礎を置く文書をサービス・プロバイダーの管理下に置く者は、文書が含む情報の秘匿性に従って当該文書により要請されるプライバシー保護に関し、および当該文書にアクセスする権利を有する者に関して、事前にサービス・プロバイダーに知らせる事を要請される。

当該文書がサービス・プロバイダーの管理下にある期間を通じて、サービス・プロバイダーは、合意された技術手段が文書のセキュリティを確保し、完全性を維持するため、および適用可能な場合には、秘匿性を保護し、無権限者のアクセスを防止するため、適切であることを示すことを要請される。

同様に、サービス・プロバイダーは、当該文書の保持に関し、法により規定されるその他いかなる義務の遵守を確保しなければならない。

第３６条　接続業者として行為し、もっぱら技術に基礎を置く文書の伝達だけのコミュニケーション・ネットワーク・サービスを提供するサービス・プロバイダーは、伝達の効率性に必要とされる時間の通常の伝達過程を通じて伝達され、または保管された当該文書を利用してなされるサービス利用者の行為に責任を負わない。

但し、特にサービス・プロバイダーが、
（1）文書の送信者となることにより、
（2）文書内の情報を選別、または変更することにより、
（3）文書の伝達、受信、またはアクセス権を有する者を決定することにより、または、
（4）文書伝達に必要以上の期間、文書を保管することにより、
サービス利用者が行う行為に加わる場合には責任を負うこともありうる。

第３７条　接続業者として行為し、コミュニケーション・ネットワーク経由で、提供される伝達サービスの一部として、当該情報へのアクセス権を有する者への後の伝達の効率性を確保するだけの目的で、技術に基礎を置く、依頼者により同ネットワークに与えられた文書を維持するサービス・プロバイダーは、そのような文書を使用して行われるサービス利用者の行為に責任を負わない。

但し、特にサービス・プロバイダーは、
（1）第３６条第２項に特定されているように、
（2）文書へのアクセス条件を遵守しないことにより、
（3）文書にアクセスした者の確認を妨げることにより、
（4）当該文書がネットワーク上の当初の場所から引き上げられていること、当該文書へのアクセス権を有する者がアクセスできないこと、または当該文書はネットワークから引き上げられるべきこと、または当該文書へのアクセスがブロックされるべきことを権限を有する当局が命じたことに気付いた後に、ネットワークから文書を引き上げること、または文書へのアクセスをブロックすることを怠ったことにより、
サービス利用者が行う行為に加わる場合には責任を負うこともありうる。

第２６条が示すように、情報セキュリティ、完全性、および秘匿性を確保し損ねたサービス・プロバイダーは、そのような方法が必要であることが警告されない場合にだけ責任を負うと判示されよう。サービス・プロバイダーが第３７条に述べられているような文書のへアクセス条件を遵守しない場合にも責任問題が発生しうる。

3.2.3 主体的側面(Subjective aspect)

情報セキュリティに対する侵害があった場合に、被害者から責任を追求され得る当事者についてあげて下さい。

具体的に以下の例について記述して下さい。

- o ハッカー(脆弱性に対して攻撃するソフトウエアを開発し、意識的に配布するもの)
- o 脆弱性の存在するハードウエアまたはソフトウエアの製造業者または開発者
- o コンサルタント、システムインテグレーター、配布者、販売業者、その他脆弱性有る技術を推奨したベンダー
- o セキュリティの評価やセキュリティ脆弱性の回避を委任されたコンサルタント
- o 脆弱性を発見する監査人
- o 攻撃を抑止するように依頼していたセキュリティ・プロバイダー
- o アプリケーションを最新に、パッチを宛ててもらうことにしているアプリケーション・サービスプロバイダー
- o システムをアウトソースしている場合のホスティング会社
- o 攻撃を許容し、または、停止し得なかったISP
- o 脆弱性を発見していながら、それを被害者、ベンダーまたは公に報告しなかった者

上述のように、ケベック州法に基づけば、責任は、その者の過誤、すなわち過失行為が、求められている補償に対する損害に寄与するすべての者の間で連帯される。当事者の過失が寄与していると認定されるためには、当該過失が損害を生じることが客観的に可能でなければならず、また当事者の行為の帰結が、当該当事者にとって通常予見可能でなければならない。[xxv] 結論として、上記のすべての当事者は技術的には責任ありと判示されうる。ただし、いくつかの問題は、それぞれの潜在的債務者に言及される意味がある。

ハッカー：言及されなければならないことは、カナダ刑法に基づけば、ウイルスまたはその他の害意あるソフトウエアを制作及び頒布すること、そのものは、刑事犯ではない。刑事的に有責であると認定されるためには、害悪を生ずる意思がなければならないか、または、刑事法典第３４２．２条(１)に述べられるように、「器械、デバイス、またはコンポーネントが、現に使用され、または犯罪遂行のため使用されることが現在または過去に意図されたとの合理的な推論を惹起する四囲の状況」が存在しなければならない。これらの事実は重要である。というのもケベック州法に基づけば、刑事責任は自動的に民事請求への門戸を開いているからである。[xxvi] いずれにせよ、前述の一般的議論において既に示したように、意図的または故意の侵害は民事責任につながる。

ハードウエア製造業者：上述のように、ハードウエア製造業者は、「同人が当該動産を製造、頒布、または供給した時点の知見状態に従えば、欠陥の存在は知り得なかったこと、および同人が当該欠陥を知るに至った時に情報を提供する同人の義務を怠っていないことを同人が立証する場合には、」[xxvii] 補償責任を負わず、また、「被害者が当該欠陥を知り、または知りえたこと、または当該侵害を予見しえたこと」[xxviii] が証明される場合にも、責任を負わない。この最後の道は製造業者にとって非常に興味深いであろう。というのはコンピュータ・セキュリティ侵害は不幸にもすべてあまりにも共通である。このことは、裁判所を説得して、それを予見可能と考えさせるだろう。しかし、ソフトウエアが安全性を約して売られている場合には、責任問題は契約法上の問題となる。[xxix]

販売業者：ケベック州法に基づけば、販売した物が欠陥製品である場合には、販売業者には、製造業者と同一の義務がある。[xxx] したがって、読者はハードウエア製造業者に関するコメントを参照のこと。

監査人：監査人の責任は、一般的権限同様、契約条項により決せられる事は明らかである。ある監査人が、合理的かつ勤勉な監査人であれば指摘したはずであった欠点に気付き損ねる場合、監査人の責任は訴えられる。それ以外の場合には、監査人の契約が、監査がシステムの欠点を１００％検出することを保証しているのでなければ、システムが後に攻撃されても責任を負わせることは困難である。

セキュリティ・プロバイダー：セキュリティ・プロバイダーの責任は産業界の標準と同様、契約条項によって決せられる事は明らかである。あるセキュリティ・プロバイダーが、合理的かつ勤勉なセキュリティ・プロバイダーであれば補修したはずであったセキュリティ・ホールを補修し損ねる場合、その責任は訴えられる。それ以外の場合には、彼の契約が、彼のソフトウエアは１００％有効であることを保証しているのでなければ、システムが後に攻撃されても責任を負わせることは困難である。

ＡＳＰ：ＡＳＰにはシステムを最新に保つ契約上の義務がある。ＡＳＰがその契約を遵守しない場

合、ＡＳＰは責任を負うと判示されうる。しかし、監査人同様、合理的かつ勤勉なＡＳＰであれば行わないこと、すなわち、発生以前には考えられさえしない問題点を補修しないこと、を理由として責任を負うとは判示されない。但し、契約が完全性を保証している場合はこの限りでない。

ホストおよびＩＳＰ：ホストおよびＩＳＰは通常契約で責任制限をしている。たとえ、そのようなことをしていないとしても、彼らは積極的に関与しておらず、単にアクセスするだけなので、彼らが責任を負うと判示されることは疑わしい。彼らがアクセスをコントロールし始めると、責任は一つの要因となる（前掲、情報技術への法的枠組みの確立のための法律第３６および３７条参照）。しかし、ウイルス感染からの保護をもうたうＡＯＬの最新版の場合のような新たなＩＳＰモデルであれば、セキュリティ・プロバイダーに関してのコメントが適用されうる。

脆弱性発見者：後に損害を生ずる問題に気付きながら、その損害を回避できたはずの方法で報告し損ねた者に責任を負わせるように解釈できる法律は、ケベック州にはない。

3.2.4 脆弱性の場所

以下のような脆弱性の発生個所によって、責任を問われる人が異なりますか？
- クライアント側
- サーバ側
- ネットワーク機器部分

明らかに、責任は過誤なしには立証できない。したがって、脆弱性がシステム・管理者のシステムに由来しない場合、そのような当事者を相手として責任訴訟で勝訴する見込みはない。ただし、何が起ころうと、そのシステムは第三者にアクセスされないこと、もしくは、彼自身またはクライアントの過誤のいずれによろうと、システム障害の場合には彼が単独で責任負担を引き受けることを、システム・管理者が保証すると契約条項で特記されている場合にはその限りでない。機器がシステム障害の理由である場合には、民法典第１４６５条が述べるところでは、当該機器を保有する者が、その物の自律的行為から生じた侵害を理由として責任を負う。したがって、システム・管理者は責任を負うと判示されるが､彼に過誤ある機器を販売した会社に民法典第１４７３条に基づき損害賠償請求をすることができる。

以下のようなソフトウエアの提供形態によって、責任の違いを区別しているかを解説してください。
- パッケージ品ソフトウエア（市販品）
- 個別開発品ソフトウエア
  - 外注（成果物検収 Deliverable）
  - 委託（工数検収 Labor hour）
- サービス提供に利用しているソフトウエア

ソフトウエアの提供形態は責任自体には影響を与えない。しかし、被害者に帰される責任の割合には影響する。民法典第１４７８条第２項は、「侵害が一部自身の過誤の結果である場合には、被害者は配分に含まれる」と述べる。したがって、顧客がパッケージ・ソフトを購入し、販売者のパッチ提供ウェブサイトを定期的にチェックしない場合､顧客にも自身の侵害に関して一部責任を負うと判示されよう。しかし、ソフトウエアがウェブ・サービスである場合、すなわち、販売者のウェブ・サーバ上に蓄積され、顧客によりアクセスされる場合には、顧客はソフトウエアを一切保管[xxxi]していないので、顧客にも非難の余地ありと論ずることは難しいだろう。

3.2.5 注意義務-標準(Duty of care-standard)

3.2.5.1 一般(general)

法によって情報セキュリティの基準が定義されていますか。
脆弱性の改善義務についての基準を法令等で設けているか？

法令等以外の情報も知っていれば教えてください。

責任問題になった場合に被告の過誤の有無を立証するためケベック州の裁判所が採用している注意義務標準は、合理的、分別あり、かつ勤勉な個人という標準である。[xxxii] これが意味することは、責任が取り扱われなければならない場合には常に、被告と同一の特徴を有する（すなわち、同一の経歴を有するか、または同一の一般的領域にいる）合理的、分別あり、かつ勤勉な個人が、同一の状況に置かれたならば、当該侵害を回避し得たか否かを、裁判所は自問しなければならないと言うことである。したがって、情報セキュリティ保護の注意義務標準は「合理的、分別あり、かつ勤勉なシステム・管理者であれば、そのようなセキュリティ・ホールを修復したか？」となる。この質問に対する答えが積極的なものであれば、責任を負わなければならない。

3.2.5.2. 管理者の義務 (Duties of administrators)

システム管理者が、不具合を修正するためになすパッチやソフトウエアを使用することを怠った場合、責任があるか。

そうするように指示された場合に欠点を補修するため、知られたパッチを使用し、またはソフトウエアをインストールし損ねた管理者は依然勤勉、分別あり、かつ合理的であると論ずることは技術的には非常に困難である。したがって、民法典第１４５７条（または関係が契約上のものである場合には第１４５８条）に基づき、多分責任が発生する。さらに、パッチは通常無料なので、熟練専門家方式の原則[xxxiii] を考慮すると、[xxxiv] パッチを使用しないことを法的に正当化する方法はないと考えられる。

しかし、コストは金銭的なものに限らない。与えられたパッチがシステム上に有する影響もまた考慮しなければならない。[xxxv] したがって、おそらく、修正がシステムおよび結果的にクライアントの利益になることを完全には信頼していないという理由で、自動的にパッチを当てないシステム管理者に関してはより複雑な問題を提起する。[xxxvi] 彼らは、その指示を「すべて合理的なパッチをインストールせよ」または「システムの適切な運用に合致するすべての必要なパッチをインストールせよ」と解釈するらしい。[xxxvii] 指示が柔軟性を増せば増すほど、後に、それらのパッチが有益である事、及び、パッチをインストールしないことが侵害を生じたことが立証された場合に、管理者の責任を判断することはますます困難になる。

システム管理者がセキュリティ情報を収集するのを怠ったとき、責任があるか。

この回答は情報の可用性による。管理者が、可用でありかつよく知られた情報に気付かない場合、彼は勤勉でなく、従って過誤がある。しかし、最も勤勉な管理者であってもあらゆる研究、白書、及びこの領域について書かれたすべての本を読んでいると期待することはできない。[xxxviii] この種の事件は最終的には証人の信用性により判断されよう。当該情報がその分野でほぼ共通の知識であることが立証されれば、管理者が良く知っている状態にないことに過失があると裁判官は考えるだろう。しかし、当該情報が漠然としており比較的新しい場合には、過失を推論することはかなり困難だろう。

これを別の方法でいうと、「可用かつ受容されている技術を利用し損ねる当事者は、そのような懈怠は合理的な注意を払う義務に違反するという理論に基づいて責任を負うと判示されることになる。」[xxxix] この一文のキーワードは「受容されている」である。不幸にも、ケベック州の裁判所は、コンピュータ・セキュリティおよびコンピュータ・ウイルスに関して「受容されている技術」問題をすでに取り扱わなければならない。

情報技術に関する事件で法が沈黙している場合は常に、ケベック州の法律家は、他所の同僚と同様、通常、他の法領域の類推に訴える。[xl] しばしば、裁判所はそのような比較に用心深くあったけれども、[xli] この技法は非常に有効であることが明らかとなった。コンピュータウイルスはしばしば、法学者とコンピュータ専門家の両者により、生物学上の同名のものに喩えられてきた。[xlii] 細部に立ち入ることなく、コンピュータ及び生物学上のウイルスの類似性は多く、[xliii] 予防すべきか、または治癒すべきかという、「治療」の比較には強力な立証を行っている。この概念を維持しつつ、ベラードギュレット対メウー事件判決[xliv]で説明されたように、医師は、実験段階にある治療を提案しない

ことを理由に責任を負うとは判示されない。大まかに翻訳すると、裁判所の意見は次のように読める。すなわち、「被告の行為は、空想的なものに関して評価されてはならず、むしろ、その期間の良い医師の行為標準に照らして評価されるべきである。」[xlv]

コンピュータの文脈に引き返すと、これが意味することは、システム管理者はパッチが可用になるや直ちに、または、パッチを発見するや直ちに、すべてのパッチを自動的にインストールする必要はない。これは常識に反するようだ。しかし、管理者は可用な技術の評価につき良く知っている状態になければならず、また管理するシステムを業界標準と調和させ続けなければならない。[xlvi] 当然、医療現場とコンピュータ技術との間の比較は不完全である。というのもコンピュータ技術はしばしばより速いペースで進化する（すなわち、パッチは医療が可能とするより早く開発される）。このことが意味するのは、システム管理者は、医師がなすよりもより早く新技術に対応しなければならないことである。それにもかかわらず、医療との類似は、裁判所は多分どのようにコンピュータ分野の責任を評価するかについての一般的考えをわれわれに与えている。

3.2.5.3 インシデントにおけるシステム管理者の義務（Duties of system administrators in case of incidents）

インシデントに対応する際、システム管理者は、不十分な対応しかできなかった場合、または、対応がおくれた場合、責任を負うか。

対応の遅れを理由とする責任は、勤勉かつ合理的なシステム管理者であれば速やかに対応すべきであるから、最も起こりやすい問題である。不十分な対応に関しては、責任は、当該不十分さがシステム管理者の側の勤勉さの欠如に帰することが出来るか否かによるだろう。問題が新しくかつ解決策が内という理由で対応が不十分であれば、管理者は責任を負うとは判示されないだろう。しかし、当該不十分さが、システム管理者の過失に起因する場合には、責任を負うと判示されるだろう。

損害を回避する責任を負う当事者が他にいますか。

民法典第１４７９条は次のように明記する。すなわち、「侵害を理由とする補償の責任を負う者は被害者が回避できたはずの侵害の悪化に関しては責任を負わない。」したがって、「ウイルスに感染したが、はじめにコンピュータを手入れせずにコンピュータでの仕事継続を試みた原告は、自身の損害を緩和しておらず」、[xlvii] ウイルスの発見後の損害を理由として訴えることは出来ない。

ウイルス伝播に役割を果たした別の当事者に関して、裁判所が以前に確立していることは、個人も会社も同様に、彼らの行為が他者に侵害を生じないようにすべての通常要請される予防措置を採らなければならない。[xlviii]

3.2.5.4. セキュリティ・ポリシー(Security policies)

1 注意義務の標準として、セキュリティポリシーを必要としていますか。

ケベック州法に基づき採用されている注意義務標準は、合理的、分別あり、かつ勤勉な個人の標準であり、責任問題に関して、裁判所も立法者もそれ以外の特定化が必要であるとは考えていない。間接的に、適切なセキュリティ・ポリシーを有しない被告は、合理的、分別あり、かつ勤勉な企業であればそのようなセキュリティ・ポリシーを有するはずであることが立証でき、かつセキュリティ・ポリシーを有することで損害が回避されるか、または持たないことで過失に寄与することが立証される場合には、責任を負うと判示されるかもしれない。別の言葉でいえば、因果的結果を別にすれば、セキュリティ・ポリシーを有することは義務ではない。こういえば、情報技術への法的枠組みを確立するための法律第４章によれば、「本法の目的のため確立された、技術手続、システム、規範および標準の、国内的及び国際的水準での、調和を奨励する」ための、委員会が創設される。[xlix] 同委員会は、法に沿って企業を援助するようガイドラインを公表する。同法第６７条は、「そのガイドラインが全部または一部履行されない場合には、政府は、同委員会との審議の後、ガイドラインに代えて規

制規定を設けることが出来る」とまで述べている。しかし、まだ最初のガイドラインは公表されておらず、ガイドラインが現状にどのような影響をもたらすか推測の域を出ない。

2 保険会社や産業界の事業者協会で、ガイドラインを標準としていることはないですか。

ケベック州では、ケベック標準局(BNQ)、標準化を担当する政府設立機関、が、以下の目的のための方法を検討する産業界の専門家の委員会を率いる職務を与えられている。すなわち、

1）異なるメディアや技術間の互換性または相互運用性、もしくは、技術に基礎を置く文書の作成と署名、およびコミュニケーションにおけるそれらの利用の技術規範および標準の調和、を確保すること
2）手続の複雑さを回避すること、特に個人の同一性確認に関して、
3）証明証およびディレクトリの標準化、および証明証の相互承認を奨励すること
4）物理的、論理的または運用上の安全手段、および文書の生成から消滅までを通じて文書の完全性を確保出来る文書管理手段をとおして、技術に基礎を置く文書の完全性を保証すること
5）監査実務を標準化すること、これには、アクセス、維持、バックアップ方法、物理的、論理的および運用上の安全手段、安全登録、および文書の完全性に影響するかもしれない欠損の場合の修正がふくまれる。および
6）適切な勧告を行い、本法の適用を慫慂すること。[l]

同委員会は究極的に上述の問題に関して「到達したコンセンサスを反映した実務上のガイドラインを開発する。」[li] しかし、今日まだ、ガイドラインは公表されていない。

この課題に関する民間部門のガイドラインについては現在知らない。

3 セキュリティポリシーの実際の運用が責任に対する抗弁になりますか。

技術的には、セキュリティ・ポリシーの採用およびその遵守は、セキュリティ侵害の場合に企業が責任を負うと判示されないことを保証するものではない。しかし、注意義務標準が、合理的、分別あり、かつ勤勉な企業主またはシステム管理者という標準であるので、いかなる事件にしても、セキュリティ問題を真剣に受け止め、かつ予防措置を採ったことを立証する被告に有利に、裁判官は判断しようとするだろう。もちろん、ポリシーおよびそれが適用される方法の程度があれこれ責任に影響する事に成功するだろう。

セキュリティポリシーの実際の運用が連邦ガイドラインのようにコンプライアンスの観点から考えられていますか。

いいえ。

4　セキュリティ上の脆弱性が、セキュリティの監査および評価をしていながら、それを探知できなかった場合、その監査および評価をしていた事実は、抗弁となりえますか。

再度、いかなる予防措置も責任に対する抗弁を提供するとは保証できない。その理由は、被告がコンピュータ・システムの維持に過失があったか否か判断するのは究極的には裁判官であるから。しかし、過誤の証明には予見の立証が必要なので、[lii] 専門の監査人により発見されなかったシステムの欠陥は予見できないと主張しうる。裁判官はそのような主張を最も受け入れやすく、被告は責任を負うと判示することを拒絶しそうである（ただし、前述の議論のように、監査人が代わって責任を負うと判示されるかもしれない)。

3.2.6 その他（Miscellaneous）

1　セキュリティ・インシデントの実体を明らかにするのに有効だと考えられる法的システムはありますか

2　「内部告発者保護」や「司法取引」の法制度を有していますか。

ケベック州法にはない。

3 「内部告発者保護」や「司法取引」の法制度が、セキュリティ・インシデントの実体を明らかにするのに有効と考えられるのではないかという議論はありませんか。
われわれの知る限り、現在そのような議論はなく、近い将来もないと予想する。

４　セキュリティ・インシデントの真実を明らかにするため法制度は特に準備されていませんか。
ケベック州法にそのような制度はない。

3.3 責任有る開示の問題（Responsible disclosure issue）

1. 脆弱性に気がついたとき、気がついた人間は、会社や公的機関に報告すべき義務がありますか。
2. 報告された会社などは、これに対して対応すべき義務はありますか。また、対応をなしうる体制をとっておく義務があると解されていますか。

ケベック州法には、知られた脆弱性を製造者、公衆、または公当局に開示する義務はない。しかし、会社は、知られた脆弱性をクライアントに知らせる義務がある。[liii]

3. 産業界や政府の機関が、脆弱性がわかった際に、それに対して責任有る開示となるようなガイドラインを準備していますか。もし、準備している際は、その内容をお教えください。

われわれの知る限り、そのようなガイドラインは可用でなく、また提案もされていない。

4. 脆弱性の報告について、その内容を分析する専門的な委員などの制度が提案されていませんか。もし、議論されているのであれば、その内容をお教えください。

上記で報告のように、ケベック州政府は、情報技術への法的枠組みを確立する法律のなかで、[liv] 技術的システム、規範、および標準の調和を取り扱うガイドラインを創設するための委員会を組織するよう命じている。同委員会は情報技術の多くの異なる側面を研究するものとされ、それらには、「物理的、論理的または運用上の安全手段、および文書の完全性を保証することが出来る文書管理手段」[lv] が含まれる。これはＳＱＬスラマー事件に結びつけられていないけれども、この質問事項で強調されたような問題は、同委員会に認識されかつ議論されることだろう。上述のように、同委員会の創設の時期またはその初期の会議日程は公表されていない。

3.4 SQL Slammer の事件をきっかけに何か動きなどがありましたか？

ＳＱＬスラマー、またはケベックで実際に発生した類似の攻撃に関して、知られている議論はない。このことはおそらく、ケベックにおいてはそのワームが拡大損害を生じなかったことに帰されよう。事実、ケベック州のメディアにはほとんど取り上げられなかった。

＊＊＊

以上で分析を終了する。この意見書へのコメントまたは質問は、以下の個人にご連絡下さい。

トロント大学法学部法政策革新センター

カナダ英米法における
コンピュータ・ウイルス拡散責任

執筆：アンドレイ・エドワード（トロント大学、法学修士論文提出資格者）

プロジェクト・ディレクター：リチャード・オーウェン（法政策革新センター長）

２００３年6月

序論

日本の経済産業省は、最近のコンピュータ・セキュリティへの攻撃に対して、法的手だてが、現に有用であるか、または有用となりうるか検討している。この過程の一部が、インターネット全域でのウイルスとワームの拡散の法的意味の分析である。特に、経済産業省が問い合わせていることは、２００２年多くの国でコンピュータ・システムにかなりの損害を生じたＳＱＬスラマーのような事件から派生する法的責任である。

以下の報告書は、ＳＱＬスラマーの状況に光をあてて、カナダにおける英米法域の法を検討したものである。これはカナダの英米法域が、刑事上、民事上、および規制上の問題に責任を課すための一般原則を検討する。そこで、それらの原則を経済産業省が提起したそれぞれの質問に適用する。

この分析から明らかなことは、カナダ法はコンピュータ・セキュリティへの攻撃を限定的にしか取り扱っていないことであり、顕著なものは、コンピュータ・システムの濫用およびそれに対する無権限アクセスに関する刑事規定である。しかし、民事責任の一般原則は、コンピュータ・システム運用者に適用され、新奇な事件として知られているが、既に法的関心の対象となっているものから、コンピュータを侵害することの、または「マルウエア」すなわち、ウイルス、ワーム、トロイの木馬その他の危険なソフトウエアを拡散することの民事責任を推断出来る。

以下は、カナダの英米法、ならびにカナダの制定法および英米法域の制定法により課される潜在的責任の分析である。これは、学問的分析であり、大学の協力において準備されておりまた、仮説的な事実（現実的ではある）を取り扱っている。経済産業省は本研究のスポンサーではあるが、法学部法政策革新センター、またはトロント大学の依頼者ではないので、依頼者に対する法的助言ではない。筆者が希望することは、これらの分析が経済産業省を支援して、他の法制度のアプローチの日本側の理解を進めることであり、インターネット時代において、コンピュータ・ネットワークの効率的な利用への地球規模の挑戦が、われわれ全員のより大きな利益のため、行われている。

経済産業省質問事項

１：定義(Definition)

1.1　脆弱性を議論するにあたって、「ソフトウエア」の定義が法にありますか。

カナダ法には「ソフトウエア」の一般的に適用可能な定義はない。いくつかの制定法では、特定の言葉でないにしても、それぞれ独自の目的のためその概念を定義している。刑法典の目的が、本研究のためには適切である。他の制定法の目的は直接には関連しない。それでも、欠陥ある、または脆弱なコンピュータ・コードを理由とする責任に関する立法を記すのであれば、立法者が何をソフトウエアと考えているかに光を当てる助けになるかもしれない。

刑法典[lvi]　第 342.1(2)は「コンピュータ・プログラム」を次のように定義する。すなわち、「指示、または記述を表現するデータで、コンピュータ・システムで実行される場合に、コンピュータ・システムに機能を実行させるもの」。単体のデバイス、または相互接続され、もしくは関連づけられた複

数のデバイスの集合体で、そのうちの一つまたは複数が、(a)コンピュータ・プログラムまたは他のデータを含み、かつ(b)コンピュータ・プログラムに従って、(i)論理およびコントロールを実行し、および(ii)その他の機能を実行するものでもよい。[lvii]

オンタリオ小売り販売税法[lviii] 第 1(1)は「コンピュータ・プログラム」を次にように定義する。すなわち、「プログラム、物、データ、情報、知識、または指示で、(a)コンピュータ、機械、またはデバイスに指示または情報を与えるため利用され、かつ(b)電子的な手段その他の方法で保持または移転されるもので、第(3)項に規定される類型のプログラム、プログラムの全部または一部の利用およびプログラムの利用権を促進するよう意図された文書・・・を含むもの。」[lix]

オンタリオ小売り販売税法第 1(3)は、同法の目的のためコンピュータ・プログラムと考えられるいくつかの類型のプログラムを規定する。すなわち、「(1)コンピュータ、機械、デバイスの利用に際する問題の解決のためのプログラムで、その問題の解決のため必要な、データ処理装置への一連の自動的指示を含む。(2)コンピュータ、機械、またはデバイスが機能をコントロールし、または機能を実行すること、もしくは求められている結果を生み出すこと、およびそれを直接または他の装置を利用して行うことを可能にするかまたは生じるための指示。(3)システム・プログラム、アプリケーション・プログラム、アセンブラー、コンパイラー、ルーチン、ジェネレイター、およびユーティリティー・プログラム。(4)書かれる以前のプログラム。」[lx]

要するに、これらの定義には、本報告で検討される責任の種類に、誰を、またはいかなる行為を、含めるか、または除外するかについて助けとなるものはない。

1.2. 「セキュリティホール」「脆弱性」「不具合」について法令等で定義をしていますか。

「セキュリティホール」「脆弱性」「不具合」を定義するカナダの法律はない。

いくつかのカナダ法は欠陥品を取り扱っているが、これらは、後に、責任に関する一般的議論においてより詳細に言及される。それらは、「不具合」そのものを定義していない。適用可能な概念は、制定法よりも法学からあらわれる。

同様に情報の秘匿性を維持する必要性について立法があるが､「脆弱性」の定義によってではない。これも同様に後述する。

1.3 「セキュリティ・ホール」という用語が法令等で使用されていませんか。

連邦法にも、オンタリオ法にも、また知りうる限り他州の制定法にも「セキュリティ・ホール」という語は使われていない。

2： 責任(Liabilities)

2.1 一般的フレームワーク(General frame work)

情報セキュリティ脆弱性もしくは不具合からの責任について、定義や責任が定められていますか。

一般に、カナダ法は情報セキュリティ問題を取り扱っていない。脆弱性および不具合を理由とする責任は、判例法から生じる、すなわち、比較しうる状況における、司法判断の合理的な拡張から生じる。例外は刑法であり、それはカナダ刑法典に法典化されている。

刑事責任

刑法は、ワームおよびウイルスの蔓延を特にはまだ取り扱っていない。

コンピュータに関連する刑事責任は、刑法典第 342.1、342.2、および 430(1.1)、(5.1)条が取り扱う。攻撃の正確な状況によっては、現行刑法典の規定が適用できよう。第 342.1 条は「コンピュータの無権限使用」の罪を取り扱う。[lxi] 同条第１項は次の通り。

(1) 何人も、詐欺的かつ権利の外観なしに、

(a)直接間接にコンピュータ・サービスを受け、

(b)電磁的、音響的、機械的またはその他のデバイスの方法で、コンピュータ・システムのいかなる

機能に、直接間接に、干渉し、または干渉される原因となり、
(c)(a)または(b)に基づく犯罪、もしくはデータまたはコンピュータ・システムに関して第４３０条に基づく犯罪を遂行する目的で、コンピュータ・システムを、直接間接に、使用し、または使用される原因となり、または、
(d)(a)(b)または(c)に基づく犯罪を人が遂行することを可能にするコンピュータ・パスワードを使用、保持、取引、または他者がアクセスする事を許す、
場合には、正式起訴犯罪で有罪とし、１０年未満の拘禁刑に処するか、または略式判決で科刑しうる犯罪で有罪とする。

「詐欺的かつ権利の外観なしに」という言葉は、被疑者は単に詐欺的にだけでなく、この行為を遂行する権利があると心からの確信を持たずに行為することを要する。もし被疑者が誤解し、または自分がこの行為を遂行する権利があると心から確信している場合には、同条に基づいて有罪にはならない。[lxii]

また検討すべきは、「コンピュータ・サービスを得るためにデバイスを占有する」罪[lxiii]　である。第 342.2 条に基づけば、第 342.1 条の罪を犯すため使用することが意図されたと合理的に推断できる状況下で、機器、デバイス、またはコンポーネントを製造、占有、販売、または販売のため提供することは、違法であり、２年の拘禁刑、または略式判決の罪で有罪となりうる。[lxiv]

「迷惑」罪もまた関連する。刑法典第 430(1.1)に次のように規定される。

第 430(1.1)　意図的に次の行為をなした者は迷惑罪である。

(a) データを破壊または変更、
(b) データを無意味化、使用不能、または無効化、
(c) データの正当な利用に、妨害、中断または介入、または
(d) データの正当な利用者に、妨害、中断または介入、またはアクセス権を有する者へのデータアクセスの拒否。

この罪で有罪の者は５年未満の拘禁刑が言い渡されるか、または略式判決（より簡略な手続）で有罪とされ、それより軽微な刑に服することになる。[lxv]

注目すべき事は、刑事責任は、違法な何かをなす故意の有無による。このことが意味するのは、ありがちなのはハッカーやマルウエアの制作者にかんしてであり、害悪あるプログラムを流布するために利用される装置、ネットワーク、または大量のコンピュータを単に供与する者ではないことである。いくつかの刑事犯罪は、未必の故意、ないし行為から生じるかもしれない害悪の「意図的無視」の存在を認める。しかし、この分析においては論点でない。

契約および制定法上の責任

損害を発生させた当事者と、それを被った当事者の間に契約がある場合には、契約条項は責任の分析にとっては不可欠である。契約に基づくこの責任には二つの要素がある。すなわち、(i)表示（または不実表示)が、当事者を契約締結に誘導すると、契約の一部をなすと後に判示されるかもしれない。(ii)販売された物品およびサービスに関する条件および保証。

販売前の表示は、販売条件、またはそれに適用される保証であると考えられ、または、表示は法的責任の独立条項と解されるかもしれない。原則として、条件と保証との差異は、条件の違反は、被害当事者が契約を解除する権利を与えるが、保証違反は、被害当事者が違反を補償する損害賠償金の権利を与える。実務上、契約条項が条件かまたは保証か裁判所でいずれと判示されるか判断することはほとんど不可能である。

コンピュータ・システムの安全水準に関する陳述は、不安全により生じた損害の責任に関係する。しかし、裁判所は、取引全体を見るので、抽象的に確かに責任につながる特定の表示はいわれない。

さらに、カナダのほとんどの州は、物品販売について黙示の条件または保証に関するある種の立法をしてきた。[lxvi]　二つの基本的な制定法上の保証がある。すなわち、(a)目的適合性の保証、特に買

い主が売り主に購買理由を告げている場合、および、特に買い主が、買い主の目的のため物品の適合性を判断する売り主の専門知識に依拠している場合。および(b)「商品性」保証、これが意味するのは、当該物品が、合理的な期間中、合理的に機能しなければならないことである。何が合理的であるかは、価格、物品の類型、その他を含む事実関係による。

前者の保証の例は、オンタリオ物品販売法[lxvii] 第 15 条があり、それによると、買い主が売り主に、その物品の使用を計画する明示または黙示の目的を知らせた場合、売り主が売った物品は明示または黙示の目的に合理的に適合しているという黙示の条件がある。[lxviii]

物品販売法の黙示の保証は、両当事者間の明示の契約を通じて適用除外できる。[lxix] ただし、消費者販売はこの限りでない。[lxx] 適用除外は、明示の保証除外（たとえば、「目的適合性保証は明示に排除される」）してもよく、また、保証と矛盾する他の陳述でもよい（たとえば、「買い主は、買い主の目的への物品の適合性評価のため売り主に依拠しない。」）。

制定法上の保証は物品販売に適用されるが、サービスの販売にはされない。ソフトウエア開発合意は、サービス契約と考えられ、制定法上の保証の恩恵はない。しかし、判例法上の保証および表示は個別の事件においては議論の余地があろう。

不法行為責任

英米不法行為法は民事不法行為、すなわちある者が他者に対して犯した不法行為責任を課する。責任は一般的に、加害者は侵害された被害者に補償するという命令となる。法のほとんどは、判例集に見られる（「判例法」）。

不法行為責任は二種類の不法行為から生じる。すなわち、故意の侵害と、故意ではない侵害である。故意でない侵害は、ある種の過誤により生じなければならないが、その過誤は通常は過失である。両種の不法行為を見ていくが、焦点は過失にある。

カナダでは、コンピュータにウイルスを感染させる事による故意の不法行為遂行に関する判例法はない。このような方法で他人に損害を意図的に生じることは、予期するに、救済方法を導くだろう。合衆国では、いくつかの裁判所が、動産侵害（不法行為の一類型）の原則を用いて、スパムを受信し、または求められていないデータ収集プログラムに服する事を通じて帯域能力を減じられたウェブサイトは、不法行為で回復可能な財産的損害を被ったと認定した。[lxxi] 市場活動の構造が類似の場合には、カナダの英米法はしばしばアメリカ法の影響を受ける。

マルウエアの配布に役割を果たす他の故意の不法行為は不実表示である。これは、契約上のそれとは別に、不法行為上の訴権を構成する。したがって、表示をなした者とそれに依拠した者との間に契約がなくても、訴訟はあり得る。ネットワーク、システム、または装置が侵入に対して安全であるという虚偽の表示をなすことは、契約の有無に関わらず、それに依拠する者に対する不法行為責任にさらされる。表示は被害者に対してなされるか、または、被害者により聞かれかつ行為されることが合理的に予見されるようになされなければならない。

損害を回避するため、またはワームを回避するための適切な防止措置を取り損ねることに関して、訴訟は過失で構成される。過失は請求が認められるために証明されなければならない四つの要件がある。すなわち、

(1) 被告には、原告に対処する場合に、合理的な注意を払う義務があり、
(2) 被告は、適切な水準の注意を履行しないことで、原告に対するその注意義務に違反し、
(3) 被告の行為は、原告の侵害結果と合理的な関連があり、
(4) 原告は現実の損失または損害を被った。[lxxii]

これらの要件または要因を、行為の種類および損害の種類の分析に適用することが、経済産業省の利益となろう。

義務：先例であるドナヒュー対スティーブンソン事件[lxxiii] に従うと、被告は、その行為により影響を受けると合理的に予見されるべきすべての者に義務を負う。カナダ最高裁判所は、私法上、二当事者間に注意義務があるか否かを決定するための２段階テストを確立している。[lxxiv] ２段階テストの第１段階は、当事者間の関係が十分に近い（近接）かを決定するために用いられる。そうであれば

一方当事者の不注意は他方に損害を生じそうである。当事者の近接関係が立証され、従って当事者間には義務がある場合には、２段階テストの第２段階が、義務の範囲、すなわち誰に対して義務があるか、またはその違反から生じる損害[lxxv] を、政策的考慮事由に基づいて[lxxvi]、裁判所が制限または否定することを許容する。この種の制限は、ハーキュレス・マネジメント会社対アーネストおよびヤング事件[lxxvii] に適用され、意図された当初の目的以外の目的の使用に供された財務報告書における過失ある陳述を理由とする決定できない責任の危険を回避した。[lxxviii]

注意義務標準：注意義務標準という困難な問題を明らかにするためには証拠が審理されなければならない。CERT[lxxix] および SANS[lxxx] のようないくつかの IT セキュリティ組織があり、IT 専門家であれば、インターネットのよりよい保護のため取るべき手段を提案する。[lxxxi] カナダの裁判所は、カナダのユーザが一般的にアメリカの標準を知っているか、または、知っているはずであることが示される場合には、アメリカに基礎を置く標準に影響されるかもしれない。しかし、産業界の標準がないことが、被告がコンピュータをウイルスから保護する義務を怠ったか否か決定することを困難にしている。標準に関してはさらに後述する。

因果関係：さらに、原告が不法行為法上請求を開始できる損失を現実に被っているかを決定する問題がある。分散型 DoS（またはワーム）攻撃は、感染したコンピュータに物理的損害を現実には生じない。それは単に要求に応じるサーバーおよび IT ネットワークが溢れるにすぎず、その結果、意図された利用に供されない。[lxxxii] この攻撃によりいかなる永続的性質が失われるか示すことは困難であろう。せいぜい、このような事件での損失は、もっぱら経済的性質を有するにすぎない。

警告を怠る責任は、危険な製造物に関して負わされている。明確でないが、この義務はサービス妨害の危険、またはデータに対する危険を生じる製造物に拡張できるかもしれないが、そのような危険は十分起こりうる。ソフトウエアまたはハードウエアの製造業者または開発業者への責任を生じうる独立の不法な行為の例は、他者に販売後にその製品の不具合を開示することを怠り、その結果、相手方当事者(第三者を含む)が、それら不具合に帰せられる経済的または物理的損失を被ることである。ボー・ヴァレイに述べられているように、「製造業者および供給者は潜在的に危険な製品により合理的に影響を受けるかもしれないすべての者[lxxxiii]（販売契約の当事者でない者を含む）[lxxxiv]に警告することが要請される・・・。潜在的ユーザは製造業者または供給者にとっては合理的に予見されなければならない。（しかし）製造業者および供給者は、その製品の不適切な使用から生じうるすべての危険について全世界に警告する義務はない。」[lxxxv]

損失：伝統的に、カナダの裁判所は、純粋に経済的な損失は不法行為法上回復できないと認定してきた。[lxxxvi] これには多くの理由があるが、決定できない責任を回避すること、および契約法に基づき開始出来る訴訟の重複という理由が含まれる。[lxxxvii] しかし、カナダ国営鉄道対ノルウェー太平洋蒸気船事件[lxxxviii] が確立したことは、カナダ法において、過失行為と損失との間に十分な近接性がある場合には（義務違反の存在および損失の予見可能性という通常の要件に沿って）、[lxxxix] 経済的損失の回復が出来ることである。ここでまた、カンループ市対ニールセン事件で確立した２段階テストは、当事者間に十分な近接関係があるか否か、および何らかの政策的考慮事由が、義務の範囲、または付与される損害賠償金を制限、または否定すべきか否かを決定するために用いられる。

要するに、不法行為法に基づく経済的損失の回復が認められるのは、原告の損失は被告の独立の不法な行為から生じたことを原告が立証でき、かつ、両当事者間に十分な近接性が存在する場合である。

規制上の責任

コンピュータ装置の販売、および、インターネットを含むコンピュータ・ネットワークの運用は、カナダでは一般に規制されていない。[xc] 放送と通信の規制者、および CRTC は、インターネットを規制することを試みないことを明示に決定した。[xci] CRTC は通信キャリアのサービス品質標準を確立したが、[xcii] インターネット上なされるコミュニケーションに標準を拡張することに関心を示していない。

その他の種類の規制体制はネット上の活動にも適用され、顕著なものに、人権規則および有価証券規制があり、カナダ法で明確なことは、私人間、または私人対州、の関係に影響する法準則はオンラ

インに適用され続けることである。かくして、不法行為と契約法の議論は本レポートにおいて、オンライン上の侵害に対して利益がある。しかし、コミュニケーション活動一般の規制に適用される原則から学ぶものは現時点ではほとんどない。

以下の可能な責任理論への特別な焦点

(a) ソフトウエアまたはハードウエアに欠陥があった製造者,開発者の責任（脆弱性を調整するよう意図されたパッチの欠陥を含む）

刑事法：

製造業者、または開発業者が欠陥を有するソフトウエアまたはハードウエアの販売を意図し、それが刑法典第 342.1 条に基づく犯罪の遂行のため使用されることが意図される場合には、製造業者、または開発業者は、刑法典第 342.2 条にもとづき有罪となりうる。

欠陥あるソフトウエアの製造業者、および開発業者はまた、そのソフトウエアを利用するコンピュータ上のデータに介入することを意図した場合には、データに関して迷惑を引き起こしたことを理由に、刑法典第 430(1.1)条に基づき迷惑で起訴される。

契約法：

ウイルスに対するソフトウエアまたはハードウエアの抵抗力に関して、買い主に製造業者または開発業者がなした保証または表示は、買い主に対する契約違反で、製造業者または開発業者に責任があるとされうる。[xciii]

ソフトウエアのライセンサーまたはハードウエアの売り主も、オンタリオ物品販売法を通じて、隠れた瑕疵を有する製品を売ることにより製品の適合性または商品性に関する黙示の保証または条件に違反するとして、責任を負うとされうる。[xciv] しかし、典型的には、そのような保護は、ソフトウエア・ライセンス、または適用できる場合には、製品保証の条項により排除される。

製造業者または開発業者が、ハードウエアまたはソフトウエアのウイルスに対する抵抗力についてなした説明が隠れた瑕疵の存在で不正確なものとなった場合、その説明は、ソフトウエアの供与に関する契約条件の一部となっているか否かに関わらず、ソフトウエアのライセンシーに対して製造業者または開発業者は責任を負うとされうる過失ある不実表示と考えられる。[xcv]

不法行為：

ソフトウエアの製造業者または開発業者は、ソフトウエアまたはハードウエアの欠陥に影響されると合理的に予見すべき当事者に義務を負う。これには、直接のクライアントおよびクライアントと接触ある者が含まれよう。多くのコンピュータがインターネットに接続しており、したがって、世界中のその他のコンピュータにも接続しており、これらすべてのコンピュータは欠陥の影響を受けると合理的に予見される。しかし、ソフトウエアまたはハードウエアの製造業者のような被告が負う義務を、確定できない種類の原告にまで拡張することに判例法は消極的である。世界中への責任を回避するため、裁判所は政策的制約を持ち出しそうである。

一般的用語では、義務はそのシステムの能力を適切に陳述することである。この状況では、被告がその製品の内在的欠陥を開示することを怠ったことが、原告がその製品を使用するときに欠陥に由来する損失について被告は責任を負うとされる独立の不法行為である。同様に、そのシステムを記述、作成、または運用するに際しての過失も責任につながりうる。

しかし、システムがインターネットに接続するようデザインされている場合、カナダの裁判所は、その設備が、インターネットを基礎とする侵害に対して、他の製造業者以上には脆弱でない製造業者に広範な責任を負わせようとはしていない。この記述については本レポートの別の箇所で産業界の標準およびその合理性についての議論が優先する。また、製造業者がその設備を安全にするある特別な義務を引き受けたと裁判所に合理的に認定させる、製造業者がなす特別な表示が優先する。

(b)　「下流責任」(情報セキュリティ侵害攻撃を停止するのに失敗した最初の被害者の責任、すなわち、そのシステムが他者のシステムを攻撃するのに利用された責任-公開されたパッチを宛てるのを怠った責任や公知の脆弱性に対応するのを怠った責任)

一般的に、その侵害につき「下流侵害」および「上流責任」と言及することが望ましく思える。侵害は感染したコンピュータから（下流へ）接続するものに流れ、また、下流のコンピュータの所有者は侵害の源泉（上流）から補償を求める。

刑事責任

ウイルス頒布の故意がなければ、刑法典第 342.1、342.2、または 430(1.1)は下流の侵害に適用されない。故意が刑事責任の必要要件である。

契約責任

当事者間に契約が存する場合、契約条項が、「下流の侵害」の責任が存するかを決する。さらに「下流」（すなわちウェブサイト・ユーザ）で影響を受ける当事者に関しては、彼らと、影響されるポータルまたはネットワークとの間の契約が、関係を律することになろう。

ウェブサイトまたはネットワークのユーザとプロバイダー間で有効な警告文に特別な注意を払うかもしれない。そのような警告文の一例が、アメリカン・オンラインの利用条件である。すなわち、

> いかなる状況下においても、アメリカン・オンライン、その補助者、そのライセンサーは、本サイトの利用、または利用不能から生ずる、直接、間接、懲罰的、付随的、特別または結果損害を理由とする責任を負わないものとする。この制限は、申し立てられている責任が、契約、不法行為、ネグリジェンス、厳格責任、またはその他のいかなる基盤に基づこうとも、たとえアメリカン・オンラインがそのような損害の可能性について助言されていようが、適用される。いくつかの法域では付随的または結果的損害の除外または制限が認められないので、そのような法域におけるアメリカン・オンラインの責任は、法が許容する範囲に制限するものとする。[xcvi]

この種の包括的警告文は、あらゆる法域で法的に強行可能ではなかろう。[xcvii]　さらに、標準様式契約は、当事者間の交渉力の不均衡問題を生じ（とりわけ、消費者契約において）その強行可能性に関する疑いがある。[xcviii]

不法行為責任

3.2.1(a)における責任の議論がここに適用される。上流のウェブサイトが公開されたパッチのインストール、および知られた脆弱性を取り扱うことを怠る場合、ウェブサイトを維持する最小限の注意義務標準違反であり、過失行為に当たると裁判所に見られよう。[xcix]

多くのウイルスが多様な形態をとる、これが意味するのは、ウイルスは、新しいコンピュータに侵入するたびごとに暗号ルーチンを変更する変異エンジンを持つことである。[c]　従って、上流に感染したウイルスは、たとえ合理的な手段を取ったとしても、対ウイルス保護手段には認識されない形態を持つかもしれないが、それが違った形に変異出来たとしても、それが下流に移動するときまでには標準的な対ウイルス予防措置に認識される。これはネグリジェンス訴訟では重要な立証問題を生ずる。ウイルスは下流では検出されたとしても、上流ではされないので、上流のコンピュータに責任を課すこと、またはどのような注意義務標準を適用すべきか評価することは困難である。[ci]

また寄与過失の要素も検討しなければならない。[cii]　寄与過失の原理は原告と被告の間で過誤を配分し、被告に自身の過誤による侵害分だけを支払わせる。[ciii]　当事者が「上流責任」を主張する場合、下流の当事者は、上流の当事者を非難するのでなく、ウイルス感染を回避する適切な予防措置を自身で採るべきであったと、上流の当事者は主張するかもしれない。自身のために取る注意義務よりもより重い注意義務を他者に求めることは出来ない。自身の行為を通じての自身に対する侵害の予見可能性が、寄与過失の重要な要素である。[civ]下流の当事者がウイルス感染回避のための合理的な手段を採っていなければ、少なくとも被った損害について寄与過失に基づき一部責任を負うことになろう。

被った損害はもっぱら経済的損失とみられるが、既に論じたように、伝統的にはカナダ不法行為法

では回復されなかった。記したように、この点に関して法は変化している。加えて、前に言及したアメリカの先例が、カナダの裁判所に影響を与えたので、補償可能な損害についてより広く見るようになったかもしれない。[cv]　したがって、ウイルスのために速度低下を被り、または停止したウェブサイトは、不法行為訴訟を通じて補償可能な財産的損害を被ったことを主張しうる。

(c) システムにおける脆弱性を発見するために効果的な監査を怠った際の責任

上記で論じたと同様の刑事、契約、および不法行為責任がここでは適用される。この懈怠は、問題当事者に適用される注意義務標準に関連する。安全評価が法により要請される理由は、契約がそれを要請しているか、または予見しうる当事者に予見しうる侵害を避ける合理的に必要だからである。議論には二つの要素がある。安全評価は合理的に要請されるか？および、安全評価は実施されたが、有効にでない（すなわち、過失あり）か？

何が合理的に必要か、また、侵害を回避する他の方法は同じく受け入れられるか否かについては常に議論の余地がある。ネグリジェンスの認定を回避するため完全性の立証は必要ない。ある十分な安全評価であれば、実際生じた侵害を回避できなかったはずはない。

2.2：セキュリティ法的責任の要素(Elements of security legal liability)

情報セキュリティ、機密性、正確性、可用性と法的責任には、どのような関係がありますか。

本問は、契約または不法行為法以外の、情報が、安全に、または秘匿され、または変更されず、または可用に保たれるべき法的要件に関するものと理解する。このような法的要件を充足し損ねることは、結果的に侵害を被る者に対して、これらの要件に服する者の側に、責任を生じさせるものであるか？

一般則として、カナダ法は、法的要件に違反すると言う理由では人に民事責任を課さない。通常の不法行為法的分析が必要である。すなわち、その者は、侵害を被った者に対して義務を負っていたか、およびその義務違反は、適切な注意標準を遵守し損ねたことによるものか？争点は、コモン・ローが課していない場合に、個々の法的ルールがそのような義務を課し、またはそのような標準を設定しているか否かである。これは個別の事件における分析の問題である。裁判所であれば、以下のように問うであろう。すなわち、個々の法的ルールが確立したのは誰の利益か？侵害を被った者の利益か、一般大衆か、政府部門か、または、適切な税金監査が、当該ルールに服する情報に基づいてなされることを確保するような何らかの無関係な目的のためか？既に述べたように、裁判所は、全世界を保護する、すなわち全世界に対して過失を犯さない義務を課すことに消極的である。その者がそのルールから利益を得ることをより特定的に意図するほど、裁判所は、そのルール違反は、違反者に責任を負わせると、より認定しそうである。

したがって、明示の契約を欠く場合には、そのような義務と法的責任のつながりは、議論の対象となる。

カナダ連邦プライバシー法は、連邦財務サービス立法のように、データの安全義務、および守秘義務を含んでいる。[cvi]　しかし、立法には自身の救済条項があり、それには、公務員による捜査と、同公務員による理由を付しての裁判所への申し立てがある。同法の規定が、私人に独自の訴訟を提起する何らかの権利を付与するものか否かはまだ判断されていないけれども、現在、複数の事件が裁判所に係属中である。

現時点で記しうることは、カナダのコモン・ローは一般的には、セキュリティ、機密性（企業秘密法の限定的な分野を除く）、完全性、または可用性、という特定の名目に義務を課していないことである。インターネットにより生ずる増加した脆弱性、および電子的記録一般の使用のために、法はこれらすべての点で発展しそうであるといって良い。インターネットを通じての過失によるデータ漏洩、

またはハード・ディスクもしくはプリント・アウトの不注意な破棄を理由とする訴訟のおそれがあったのだが、既に開始された。ただし、判決はまだ下されていない。

要するに、カナダも、日本やその他の法域とこれらの問題を共有しているが、その解決までには至っていない。

2.3 主体的側面(Subjective aspect)

情報セキュリティに対する侵害があった場合に、被害者から責任を追求され得る当事者についてあげて下さい。
具体的に以下の例について記述して下さい。

- ハッカー(脆弱性に対して攻撃するソフトウエアを開発し、意識的に配布するもの)
  ハッカーは、その意図が明白なので、上述した刑法典の規定にもとづき、刑法上最も責任が負わされそうである。契約法は彼らに適用されそうもないが、不法行為法は適用されそうである。彼らの行為は予見可能な結果を有しており、予見可能性は注意義務、および損害賠償金算定の要素である。もちろん、しばしばハッカーの発見は困難であり、それが理由で、人は被った侵害を理由とする補償の源泉の他の可能性を探るのである。

- 脆弱性の存在するハードウエアまたはソフトウエアの製造業者または開発者
  製造業者および開発者の責任は既に論じた。刑事責任はありそうにない。契約責任は、保証および恐らく表示にもとづき、より可能性があるが、契約が責任を排除しそうであり、そのため免責条項の強行性に関して争点がある。不法行為責任も、製造業者または開発業者と、被害者との間に契約がある場合には、契約で免責されうる。契約がない場合には、既に知られ、または知られるべきであった脆弱な装置の製造業者に、予見可能な被害者に対する責任を法が負わせてしかるべきである。この責任は、被害者が侵害を避けるための合理的な手段を採り得たはずである場合には、被害者の側の寄与過失を理由とする縮減に服する。

- コンサルタント、システムインテグレーター、配布者、販売業者、その他脆弱性有る技術を推奨したベンダー
  これらの当事者は、その推奨が侵害を生じると合理的に予見される場合には、推奨を理由とする民事責任があってしかるべきである。その責任は、製造業者の責任と同様であり、契約または不法行為により生じうる。裁判所は、ネグリジェンスの通常の基準を適用するだろうが、責任は厳格責任ではない（すなわち、ネクリジェンスがなくとも課される）。当事者は何を知っており、または何を知っているべきであったか？

  加えて、裁判所はこれらの者と、(あるのであれば)侵害の被害者との契約を検討するだろう。コンサルタント（等）は発生した種類の侵害を回避する専門性または能力を有する者として自身を提供したか？その場合には、裁判所はより進んで、彼らにその侵害の責任有りとし、表示に矛盾する免責条項を無視さえするかもしれない。

- セキュリティの評価やセキュリティ脆弱性の回避を委任されたコンサルタント
  これらの者は上述の者と同一の立場にあるが、一点異なる。彼らは、自身をコンピュータ・セキュリティの専門家として提供している。したがって、彼らは、より高度な注意標準を充足しなければならない。別の言葉で言えば、小売業者にとって合理的であり得るものも、セキュリティ・コンサルタントにとっては合理的ではないかもしれない。セキュリティ・コンサルタントは、脆弱性に関してはより最新の状態を維持しなければなるまい。裁判所は事件ごとに事実を考察するだろう。

- 脆弱性を発見する監査人
  監査人は、その職責が明らかに脆弱性の発見である場合には、セキュリティ・コンサルタントと同一の立場にある。この文脈において、脆弱性の源泉の問題を検討する他の人たちも想起される。たとえば、公開市場に株式を上場する観点、または会社売却の観点から、会社を検討する法律事務所がある。専門性の程度および誰かに対して危難を開示する義務は、事件ごとに多様であろう。

- 攻撃を抑止するように依頼していたセキュリティ・プロバイダー
  攻撃に対応する責任を有する者（企業）は、その専門性に相当する注意標準、およびそのサービス契約においてなされる表示（上述のように、免責条項に服する）に従って判断されよう。

- アプリケーションを最新に、パッチを宛ててもらうことにしているアプリケーション・サービスプロバイダー
  これらの当事者も、前の者と同一の立場である。彼らが、明示または黙示に引き受けた責任、および、生じた損害は、彼らの責任を充足し損ねたことに帰することが合理的であるか否かを、分析する必要がある。

- システムをアウトソースしている場合のホスティング会社
  この当事者も前述と同一の立場にある。

- 攻撃を許容し、または、停止し得なかった ISP
  一般的には、仲介業者は責任を負わない。ただし、別表示の場合を除く。契約条項および産業界の実務が重要であろう。ISP が仲介業者と認められる場合には、通常の不法行為法分析が適用されよう。被害者のサービスをホストする ISP の立場は、ノードとなりネットワークのポイントを中継する一般的業務の一部として危険なメッセージを単に伝送する ISP よりも、恐らく責任有りとされやすい。

  注目に値することは、一般通信事業者（電話会社のような）は、一般的には彼らが伝達するメッセージの中身を理由とする責任を負わないことである。ただし、彼らが、メッセージが違法または有害なことを知るに十分な理由がある場合にはこの限りでない。ISP は一般通信事業者であるとまだ認定されていないが、カナダにおける大手 ISP のいくつかは、電気通信事業者により運営されている。

- 脆弱性を発見していながら、それを被害者、ベンダーまたは公に報告しなかった者
  カナダのコモン・ローでは、切迫していても自身引き起こしたのでない危害を誰かに警告する一般的義務はない。ただし、そのような義務は契約またはその他公的立場により生じうる。（州は、場合により、規制者としてそのような義務を有するかもしれない。しかし、最近の司法判断では、規制当局の規制に服する不法行為者により侵害された場合に、規制当局の責任を否定した。その義務は、不法行為の特定の被害者に対してでなく、一般大衆に対するものであるといわれる。）

2.4 脆弱性の場所

以下のような脆弱性の発生個所によって、責任を問われる人が異なりますか？

- クライアント側
- サーバ側

- ネットワーク機器部分

脆弱性の場所は、刑事法においてはほとんど違いがない。責任は当事者間の契約関係、および機器が使用されている目的に主に依存しそうである。その目的は契約に含まれると理解される危険の範囲を決定しうる。

場所は、またネグリジェンス（すなわち、不法行為）でもほとんど違いがない。ただし、損害の予見可能性、および被告に損害回避の責任を負わせる合理性に影響する程度を除く。この争点に関して一般化は出来ない。

ネットワーク・サービス・プロバイダーは、技術産業界における立場から信頼されているために、より重い責任の危険に直面しうる。さらに、より高い注意標準が一般的には、消費者よりも、コンピュータ・サービスのプロバイダーに適用されよう（但し、プロバイダーのように取り扱われるべき、内部的専門知識を有し、かつ公のネットワークに対する公開を、特定のエンド・ユーザがなしている状況が想起されうる。）

以下のようなソフトウエアの提供形態によって、責任の違いを区別しているかを解説してください。
- パッケージ品ソフトウエア（市販品）
- 個別開発品ソフトウエア
  - 外注（成果物検収 Deliverable）
  - 委託（工数検収 Labor hour）
- サービス提供に利用しているソフトウエア

提供形態は、契約に基づく責任、特に、品質（セキュリティ等）表示の範囲および強行性、ならびにソフトウエアの保証の性質に最も影響を及ぼしそうである。契約がより特定的であるほど、——すなわち、顧客の特別な使用目的のためのソフトウエア開発の一人のための特別契約を一方の極とすれば、大規模市場既製ソフトウエアが他方の極となる——
一層、裁判所はソフトウエアが侵害を生じないことを求めそうである。もちろん、専門的買い主は、売り主の専門的知識に依拠する必要がある買い主ほどには、この保護から利益を得ないかもしれない。

もちろん、契約の常として、免責条項の文言と強行性は争点である。

さらに、ソフトウエアがある特定の目的またはある特定の当事者を意図する場合に、意図された以外の当事者に、または意図された目的以外の何かに損害が生じた場合、ソフトウェアの供給者は、それらの損害に責任を負わない。[cvii] この場合、責任は契約でなく不法行為であり、通常の不法行為原則が適用される。

2.5 注意義務-標準(Duty of care-standard)

この節は、自らのコンピュータにより生じた侵害の被害者に対する注意義務があると法上認定される者に適用される注意標準に当てられると理解する。

2.5.1 一般(general)

法によって情報セキュリティの基準が定義されていますか。
脆弱性の改善義務についての基準を法令等で設けているか？
法令等以外の情報も知っていれば教えてください。

情報セキュリティ保護の注意標準を定義する法律はない。ソフトウエアの脆弱性を修復する義務を特に規定する制定法はない。しかし、判例法では、製造業者および供給者は危険な製造物により潜在的に影響を受けるかもしれない人に警告する義務を確立している。[cviii]前述のように、CERT および

SANS のような情報技術セキュリティ組織があり、IT 専門家であればそのネットワーク防衛のため従うべき最善の実務を推奨するが、強制的な最低限度の標準は存在しない。[cix] そのような問題は、裁判所が、専門家である当事者に相応しい注意標準、および被告の義務を判断するため、産業界の専門家から証拠を聴取する問題である。

ありそうなことは、保険会社が最も適切な注意標準を定立するに至ることであり、また最も効率的標準は、最小危険のプロセスであるが、その理由は、人の行為に対して、合理的な掛け率で保険を得る能力は、保険業者が決するものに従うことに依拠するからである。これは確かに、多くの他の産業における状況である。火災消化システムの一般利用を想起すると、使われているのは、公法が要請しているからでなく、保険業者が要請しているからである。しかし、今までのところ、保険業者により課される特定のコンピュータ・セキュリティ標準は知らない。これは、比較的速やかに発展しそうであるから、注意が払われるべき領域である。

5.2. 管理者の義務 (Duties of administrators)

システム管理者が、不具合を修正するためになすパッチやソフトウエアを使用することを怠った場合、責任があるか。

明示の指示に従わなかった管理者は、指示に従っていれば避けられたはずであった侵害を理由とする責任を負うことになりそうである。その指示が時宜を得た方法で合理的には従うことが出来なかった理由を証明することは管理者には許されよう。管理者にどれだけ独立の判断の余地があったかを知ることが適切であろう。管理者に独立性が乏しいほど、指示に従わなかった抗弁が少なくなる。不法行為法の常として、寄与過失は管理者の過誤を理由とする損害を制限する要因となりうる。[cx]

システム管理者がセキュリティ情報を収集するのを怠ったとき、責任があるか。

管理者が自身の判断権を公使する場合、過誤の立証は一層困難になるかもしれない。コンピュータの領域では、多くの安全警告があり、そのすべてについて行き、優先順位を設定することは難しい。さらに、あるセキュリティ・パッチは、多くのソフトウエア・パッケージを組み合わせた複雑なオペレーション・システムに介入するかもしれず、管理者は、ある時には一定のパッチをインストールしないと判断することが合理的かもしれない。責任は、特定のパッチが可用で、知られており、かつインストールしても合理的に無害であることの証明に依拠する。

システム管理者の過失行為が、代位責任を通じて管理者の雇い主に責任を負わせ得ることに注意すべきである。カナダでは、雇い主は次の二つの状況で代位責任を負う。すなわち、（1）被用者の行為は雇い主が権限を与えている場合、または（2）権限ある行為に結びつけられて、権限を与えられた行為をなす態様（不適切な態様であろうと）と見られ得る権限を与えられていない行為。[cxi] 逆に、管理者は個人的に有責となりうるが、ありそうにないが、これらの事実に基づき、ほぼ間違いなくもっぱら雇用されている最中に管理者は行為していたはずであり、雇い主は選択的当事者となる。

雇い主とシステムのユーザ（侵害の被害者）間の、サービス契約における、免責条項、権利放棄、または責任制限は、雇い主を保護すると同様に、システム管理者の行為を理由とする個人的責任から管理者を保護するために管理者に拡張されうる。[cxii]

5.3 インシデントにおけるシステム管理者の義務（Duties of system administrators in case of incidents）

インシデントに対応する際、システム管理者は、不十分な対応しかできなかった場合、または、対応がおくれた場合、責任を負うか。

対応の遅れおよび不十分は、それぞれ注意標準違反である。注意義務が立証され、かつその不行動が注意標準違反であって、損害を生ずるか、または損害を回避し損ねたことが示された場合には、責

任を生ずるに十分であろう。

さらに被害者の管理者は､管理者の不行為を理由とする寄与過失を管理者の雇い主に追及されうる。したがって、被告の過失に帰されると認定されるかもしれない、管理者またはその雇い主の損害賠償金は、管理者の寄与過失により減額または排除されうる。[cxiii]

損害を回避する責任を負う当事者が他にいますか。

カナダ法は一般に､侵害を被った者がその侵害を緩和するための合理的な手段を採ることを要請する。これは、実際上関係があるが、寄与過失法とは別の概念である。緩和し損ねることは、過失には当たらないだろうが、にもかかわらず、法上補償される損害賠償金を減ずるかもしれない。[cxiv]

5.4. セキュリティ・ポリシー(Security policies)

1 注意義務の標準として、セキュリティポリシーを必要としていますか。

2.2 節ですでに述べたように、連邦プライバシー法および連邦金融組織法のような、いくつかの特定の法律は、データの安全を提供するポリシーを組織が採用することを求めている。そのようなポリシーは、またはそれらを適切に定式化するか、または維持することを怠ることは、確かに、適切な注意標準を決定し､それが違反されていたか否かを決定することに一定の役割を果たすだろう｡しかし､上述のように、制定法は、制定法上の義務違反を理由として民事訴訟を提起する直接の権利を与えるものではない。

2 保険会社や産業界の事業者協会で、ガイドラインを標準としていることはないですか。

上述 2.5.1 節への回答参照のこと。そのような標準を実際に執行していそうな協会の調査をすることなく権威的な回答をするのは難しい質問である。しかしながら、既に述べたように、私的な標準が設定されるだろうことは、この問題に適切でありそうである。銀行間ネットワークおよびクレジット・カード協会を含む、金融サービス産業は、安全なデータ交換標準が充足されることを現に求めている。一時的な救済方法は、ネットワーク契約に従う構成員に限定されており、ネットワーク標準の遵守または不遵守により影響を受ける契約外の当事者には拡大されていない。

3 セキュリティポリシーの実際の運用が責任に対する抗弁になりますか。

セキュリティ・ポリシーの遵守はネグリジェンスを理由とする訴訟への抗弁には関連性を有する。確かに遵守しないよりも遵守する方が望ましい。しかし、遵守は、完全な抗弁とはならない。ポリシーそのものが適切な標準に適っているか否かが判断されよう。[cxv] ポリシーは適切なものでなくてはならず、かつ実務上その遂行が適切なものでなくてはならない。議論のあるところで、まだ先例によって判断されていないことだが、制定法において定立された義務は、いわゆるより「セーフ・ハーバー」、すなわち、責任から保護するためには不適切、または不十分であるとの追及の余地が少ない、となるかもしれない。

4 セキュリティポリシーの実際の運用が連邦ガイドラインのようにコンプライアンスの観点から考えられていますか。

刑法犯が主張されている場合には、被疑者が受け入れられている手順に従ったか否かは、量刑において関連するかもしれない。しかし、想起すべきことは、刑事責任は故意の行為にしか適用されないことである。完全にセキュリティ・ポリシーを遵守する者が、同時に法違反を意図していることはありそうもない。おそらく、故意の法違反は被疑者の行為の別の局面で生じ、セキュリティ・ポリシーは、その行為の非難の程度には関係がないかもしれない。（カナダは、アメリカ合衆国において適用される種類の量刑ガイドラインを持っていない。）

先に指摘したように、カナダには、安全でないコンピューティングを理由とする規制上の責任がほ

とんどないので、規制標準の遵守は、この文脈では問題にならない。

刑事法に基づく以外の制定法上の標準に関しては、そのような推論は適用可能で、決定的ですらありえる。そのような標準は当然払うべき注意を要請する。すなわち、その場良いには、特に標準が省庁により認められている場合、標準の厳守は、思うに刑罰を避けるための適切な方法である。絶対責任要件は、適切な注意標準に従った行動によっては避けられない。この争点に特に向けられた法律はないので、依然、いかなる標準を政府が採用するかを見る必要がある。

5　セキュリティ上の脆弱性が、セキュリティの監査および評価をしていながら、それを探知できなかった場合、その監査および評価をしていた事実は、抗弁となりえますか。

抗弁に関する本問と前問との差異は、監査または評価が第三者によりなされる場合と、セキュリティ・ポリシーを遵守しつつ、脆弱なシステム自体の所有者によりなされる場合であると思われる。しかし、これに対する回答は、前問と同一である。不法行為法の一般原則が適用されるが、たとえ、損害がとにかく発生したとしても､安全原則､または安全監査は注意標準を充足しているかもしれない。

2.6 その他（Miscellaneous）

「内部告発者保護」や「司法取引」の法制度を有していますか。

損害賠償の責任、または過酷さが、内部告発者、または別の訴追に有益な情報の見返りにより低い求刑を交渉する者の立場にある何者かのために引き下げられ得るか否かを究明するのがこの質問の目的と思われる。端的に応えると、我々はそのような効果を生むような法原則を有していない。しかし、刑事問題の実務では、他のサービスの見返りに求刑を交渉することはありうるかもしれない。検察が協力的被告により低い量刑を求める、量刑における取引は、裁判所に開示されなければならないが、裁判所は取引には拘束されない。いかなる求刑がなされるかは検察の自由裁量の問題であり、一般には公にはされない。

連邦プライバシー法は、雇い主が個人情報を保護していないと信じ、かつそのことを連邦プライバシー・コミッショナーに通知する被用者に内部告発者保護を与えている。[cxvi] オンタリオでは、内部告発者保護制度は、州政府の不法な行為の陳述の開示を理由として、被用者（州政府）の報復から、州政府の被用者を保護するために利用される。[cxvii] いずれの場合にも、内部告発者自身の不法な行為を理由として内部告発者に適用される刑罰を軽減することを、制定法は明示に認めてはいない。

「内部告発者保護」や「司法取引」の法制度が、セキュリティ・インシデントの実体を明らかにするのに有効と考えられるのではないかという議論はありませんか。

前問で回答済み。知る限り、そのような種類の関連性も最近の議論もない。

セキュリティ・インシデントの真実を明らかにするため法制度は特に準備されていませんか。

セキュリティ・インシデントの開示責任を取り扱う、直接の法律はないが、3 節の第一問への回答に注意せよ。

3 責任有る開示の問題（Responsible disclosure issue）

脆弱性に気がついたとき、気がついた人間は、会社や公的機関に報告すべき義務がありますか。

カナダ判例法における、ソフトウエアの脆弱性を結果的ユーザに開示する義務に関しては、上述2.1 節を参照のこと。また、製造物責任法にもとづき、ひとたび、製造業者がその製品の欠陥を認識したなら、注意標準は劇的に増加し、彼らが行動をとる誘因となる。

現在、インターネット・ワームの多くの攻撃は報告されていないように思われる。その理由は、多くの会社被害者は、それらの攻撃のうちのひとつの被害者になることに伴い、顧客および株主に、悪評、および否定的影響を受けることを望まないからである。[cxviii]

しかし、公衆へのセキュリティ提供を律する法は、公的会社は、公衆に時宜に適った方法で重要な事実を開示するよう求める。これが適用されるのは、公衆に株式を提供する際に目論見書を発行するときだけでなく、その後、株式が公に取り引きされる時もである。重要な事実は、もし知られていなければ、株主または潜在的株主の投資判断に影響しそうな事実である。深刻なコンピュータ・セキュリティ問題が重要な事実を構成することは非常にありうる。しかし、この法制度に基づき開示された特定の問題については、知らない。これに関する発展を遠からず見ることになりそうである。

産業界や政府の機関が、脆弱性がわかった際に、それに対して責任有る開示となるようなガイドラインを準備していますか。もし、準備している際は、その内容をお教えください。

連邦および州政府のいずれも、知られた脆弱性の責任ある開示のためのガイドラインを有していない。そのような方策についての議論もない。私的な議論については分からない。

CERT がそのようなガイドラインを有していることに注目すべきである。CERT の知られた脆弱性の開示のためのガイドラインは、http://www.kb.cert.org/vuls/html/disclosure で利用できる。CERT はアメリカの機関であるが、カナダでも知られて、敬意を払われており、カナダの裁判所は、開示が原告への損害回避に役立ったはずの不法行為訴訟のおいて注意標準を評価する場合には、それに注目してしかるべきである。

脆弱性の報告について、その内容を分析する専門的な委員などの制度が提案されていませんか。

公的または私的な部門のいかなるレベルでもそのような委員会については知らない。

4　SQL Slammer の事件をきっかけに何か動きなどがありましたか?

2001 年、カナダ政府は、重要インフラ保護および緊急対策局（OCIPEP）を創設した。[cxix]その機能の一つは IT の脅威または脆弱性に関する警告、助言、および情報を提供することである。OCIPEP はそれら IT の脅威または脆弱性に関する認知を上げ、情報を広げる。[cxx]カナダにおけるワーム防止に関して、OCIPEP による特定の議論はないが、OCIPEP は、SANS のような国際機関と協調し、インターネットがウイルスにより耐性を持つよう支援している。[cxxi]

コミュニケーション・セキュリティ・エスタブリッシュメント（CSE）[cxxii] はもう一つの連邦政府機関で、カナダ政府の情報および IT ネットワークのセキュリティを保護するよう働いている。 その機能のいくつかには、連邦政府の IT・セキュリティ・ポリシーの開発、および IT 製品の脆弱性の分析が含まれる。[cxxiii] しかし、それらの活動が、私的部門の組織に適用されることにはほど遠い。公正に言って、標準の全問題は発展中であり、公的部門に適用される標準と、私的部門に適用される標準との差は少なくなっているようである。

5　「ソフトウエアの脆弱性に対応するガイドライン」の観点でご意見があれば教えてください。

見つけられる唯一のガイドラインは、CERT であり、http://www.kb.cert.org/vuls/html/disclosure にある。カナダには直接これに対応するガイドラインがないと思われる。

（了）

註については、添付のオリジナル報告書の脚注を参照のこと。

i

ii

iii

iv

v
vi
vii
viii
ix
x
xi
xii
xiii
xiv
xv
xvi
xvii
xviii
xix
xx
xxi
xxii
xxiii
xxiv
xxv
xxvi
xxvii
xxviii
xxix
xxx
xxxi
xxxii
xxxiii
xxxiv
xxxv
xxxvi
xxxvii
xxxviii
xxxix
xl
xli
xlii
xliii
xliv
xlv
xlvi
xlvii
xlviii
xlix
l
li
lii
liii
liv

lv
lvi
lvii
lviii
lix
lx
lxi
lxii
lxiii
lxiv
lxv
lxvi
lxvii
lxviii
lxix
lxx
lxxi
lxxii
lxxiii
lxxiv
lxxv
lxxvi
lxxvii
lxxviii
lxxix
lxxx
lxxxi
lxxxii
lxxxiii
lxxxiv
lxxxv
lxxxvi
lxxxvii
lxxxviii
lxxxix
xc
xci
xcii
xciii
xciv
xcv
xcvi
xcvii
xcviii
xcix
c
ci
cii
ciii
civ

---

cv
cvi
cvii
cviii
cix
cx
cxi
cxii
cxiii
cxiv
cxv
cxvi
cxvii
cxviii
cxix
cxx
cxxi
cxxii
cxxiii

『セキュリティホールに関する法律の諸外国調査』報告書

付録　Ｂ－３

フランス　報告書日本語訳

（余白）

情報セキュリティの責任に関する問題

経済産業省のためのレポート

Valérie SEDALLIAN Avocat à la Cour de Paris

I.任務の内容

提示された事例は、Slammer 事件を念頭に置いたもの、要するにウィルス等の被害をインターネット経由で受けた者がその発信元の責任を追及したが、発信元もまた被害者であること、発信元はウィルス対策を十分に施していなかったことの責任があるかどうか、またアプリケーションの製造者に責任があるかどうか、という問題である。

具体的な回答の前に、フランスの情報システムセキュリティに関する法的枠組みを簡単に紹介する。

II. フランスの情報システムセキュリティに関する法状況

2.1 刑事責任

刑事責任は原則として検察官によって訴追される。

しかし犯罪の被害者は自ら刑事訴追を開始する可能性を有し、または司法機関に調査を開始させることができる。また、附帯私訴を提起して損害賠償を請求することができる。

今回の設例でも、刑事犯罪 infraction pénale を構成するのであれば、被害企業は告訴と附帯私訴による損害賠償をなし得る。

2.1.1 電子計算機詐欺 Fraude informatique

刑法典 323-1 条ないし323-7 条は電子計算機詐欺の罪を定める。特に、323-1 条はコンピュータシステムへの詐欺的な侵入、管理行為を、323-2 条はコンピュータシステムの機能を妨げたり誤らせたりする行為を、323-3 条はデータを詐欺的に入力したり修正削除したりする行為を、それぞれ罰している。

フランスの裁判所はコンピュータウィルスのシステムへの侵入を最後の条項に基づいて罰した。

伝統的に、システムが保護されていることは処罰の要件とならないと考えられている。

今回の設例でもウィルス作者はこの規定により処罰されうる。

ウィルスをばらまいてしまった企業やそれを許してしまったアプリケーションメーカーはどうかというと、刑事責任においては主観的要素としての詐害意図が立証されなければならない。

これまでの先例でもウィルスについてこの詐害意図は立証困難である。あるコンピュータ関連出版社がウィルス入りフロッピーを頒布してしまったという事案で担当者と取締役が訴追されたが、控訴院は重過失を認められても故意にウィルスつきのまま放置したことは認められないとして、無罪とした。被害者は被告のコンピュータとウィルスに関する十分な知識から故意が推論できると主張し、破毀院はその主張の当否を審理すべきだとして破棄差戻しを命じた。つまり技術的データの十分な知識から詐害意図も推論できるということになる。

結局、本設例についても、ウィルスの発信元について、詐害意図の立証はきわめて困難であるが、電子計算機詐欺の刑事責任を追求される可能性は否定できない。

2.1.2 保安義務

フランスには顕名情報の収集処理の中で個人データの保護を定めた法律がある(1978 年1 月6 日のコンピュータと自由に関する法律)。

この法律の顕名情報とは間接的にでも個人が特定できる情報をいう。登録番号や電話番号、電子メールアドレス、非顕名の複数の情報の集積などがこれに当たる。

同法 29 条によれば、このような顕名情報を扱う者は情報のセキュリティを確保するために有用な予防措置を取らなければならない。そしてこの義務違反は刑法典 226-17 条違反となる。

さらに 1995 年 10 月 24 日 EUディレクティブ 95/46 号も、現在フランス国内法化の作業中だが、17 条で個人データ保管責任者の義務を定めている。中でも健康、秘密の個人コード、銀行口座番号、クレジットカード番号などは高レベルの保護が要求されている。

その他にも電子的コミュニケーション分野における個人データ処理とプライバシー保護に関する 2002 年 7 月 12 日 EU ディレクティブ 2002/58 号も、4条「セキュリティ」において、電子コミュニケーションサービスのプロバイダが、回線事業者とともに、最新技術に基づくセキュリティ措置を講じる義務があること、ネットワークセキュリティに特定の危険がある場合には会員にその危険と、回避できない場合はその修復方法を通知する義務があることが規定されている。ただしこれはフランスで国内法化が未だなされていない。

しかしながら、セキュリティ保持義務違反で訴追されることはまれである。実際に有罪判決が下された例としては、労働医療組合の組合長が、必要なセキュリティを怠って、情報開示を許されていない第三者にデータを漏らしたケースが挙げられる。

そもそも刑法の条文には情報セキュリティを確保するにの有用な予防措置という概念がない。これは伝統的には手段債務であり、つまり絶対的な義務ではない。予防的な、また特有な考え方であり、事案ごとに裁判官が鑑定人の見解を踏まえつつ判断していくしかない。

フランスで個人情報保護に責任を持つ行政機関 CNIL(Commission Nationale Informatique et Liberté)は、1981 年にコンピュータシステムのセキュリティに関する一般的指針を発表した。しかしそれはまだ具体化されていない。

フランス法において、個人情報処理には CNIL に対する届出が必要で、その中にはコンピュータセキュリティ措置に関する項目もある。この届け出審査において CNIL は、処理責任者にセキュリティ強化を指示することができる。例えばインターネットを通じた遠隔医療ネットワークについて CNIL は暗号化とデータ保護の観点から、認証およびコントロールの強化を志向する見解を出している。

本設例においても、個人情報が取り扱われている限りは刑事訴追の対象となりうるが、本設例の被害者が加害企業を訴追可能かどうかは疑問である。というのも、刑法 226-17 条は当事者のセキュリティ義務違反が反射的に他者のコンピュータシステムに被害をもたらした場合を含んでおらず、刑法の条文解釈は厳格になされるべきだからである。

その上、ウィルスの被害を受けたと主張する被害企業は、自分自身もセキュリティ義務違反の批判を受けるであろう。告訴した場合、自らもまた告訴されるリスクを背負い込むことになるのである。

最後に、加害企業が被害企業の委託先であった場合（例えばホスティング業者）、フランス法はその処理の第一次責任を規定している。条文は<<データ処理を実施または実施させる行為>>を規定している。この処理責任概念は前記ディレクティブ 95/46 の 17.2 条にも見られる。

2.1.3 新規の刑事立法

現在国民議会で審議中のデジタル経済の信頼性に関する法案は、電子計算機詐欺の刑罰を重くし、手段提供に対する新たな処罰規定を設けようとしている。これによって、電子計算機の攻撃に使える道具を提供した者に対する訴追が可能となる。

コンピュータセキュリティの専門家は、この法案に基づいてウィルスの被害者が訴追される可能性があるとして、法案を批判している。

本設例においてはこの新法案の内容が重要である。ただし、ここでも詐害意図が証明されなければならない。

2.2 民事責任

2.2.1 不法行為

民法典 1382 条以下の不法行為は、契約によらない関係において、過失責任を定める。本設例においても、被害企業は加害企業がウィルス発信を防ぐに必要な措置を取らず、損害が発生し、かつ損害が加害企業の過失によって発生したことを立証すれば、責任を追及できる。

さらに 1384 条 1項は、有体物について、その管理者の不法行為責任を推定し、被告側の不可抗力または外在的原因の立証を要求している。判例はないが、学説はソフトウェアに適用がないとしている。

2.2.2 契約責任

加害企業と被害企業とが契約関係にある場合は、契約責任が考えられる。例えばホスティング契約、セキュリティ措置を行う契約、コンピュータセキュリティのアドバイスを行う契約、コンピュータシステム開発契約などである。

契約責任においては、債務の内容に関する手段債務と結果債務との区別を考えなければならない。結果債務の債務者は不履行によって直ちに損害賠償義務を負うのに対して、手段債務の債務者は最善の手段を提供しなかったことについての過失が認められる限りにおいて損害賠償義務を負う。コンピュータの供給に関する債務は手段債務と解するのが判例学説の一般的傾向であり、また多くの免責条項が契約に定められているので、故意または重過失の場合を除いて免責されることになる。

ごく最近の判例<<Chronopost>>は、債務者の本来的債務不履行を免責した契約について、契約の目的を達し得ないとして無効とした。

さらに損害の算定も困難である。

コンピュータについて、セキュリティに関する一般的約束を主張することは困難である。

逆に、契約条項が積極的な保証、メンテナンス、警告などを定めている場合、それらに違約金条項が定められている場合など、積極的義務となっている場合には賠償請求可能である。例えば本説例でも、マイクロソフトの提供する SQL のパッチをあてることが契約上定められていて、それを怠った場合などが考えられる。この場合は被告側が義務違反について不可抗力等を立証しなければ責任を免れない。

これに対して契約上も技術水準に適合したコンピュータシステムのセキュリティを施すことを約束していたにすぎない場合は、手段債務が問題となる似すぎず、原告は被告の義務違反を立証しなければならない。

結論として、責任は契約条項と給付の内容に依存する。

2.3 損害の共同責任者間の求償

民事責任でも刑事責任でも共同責任者は連帯責任を負う。

そして共同不法行為者で損害を賠償した者は、他の共同不法行為者に対してそれぞれの負担部分について求償できる。

2.4 医療データの保管の場合

患者の権利および衛生システムのメリットに関する 2002 年 3月 4 日法律 2002-303 号は、医療データ保管に関する特則をおいている。公衆衛生法典 L.111-8 条は医療データ保管を認可事項とし、CNIL の意見に基づいたデクレがその認可条件を定めるが、その中でも情報分野のセキュリティをコントロールする機構と内部コントロール手続を要件としている。ただし、デクレはまだ制定されていない。

III. 質問に対する回答

以下においては、「法」という用語を、この質問票に関するかぎり、制定法、規則、法令、判決例、行政規則などのすべての公の準則をいうものとする。

3.1 **定義**(Definition)

3.1.1. **脆弱性を議論するにあたって、「ソフトウエア」の定義が法にありますか。**

A, ない。

コンピュータ詐欺に関する規定では、コンピュータシステムを「データの自動化された処理システム」と定義している。

個人情報の自動処理に関する定義は、コンピュータと自由法 5条に定義がある。

3.1.2. 「セキュリティホール」「脆弱性」「不具合」について法令等で定義をしていますか。

A. セキュリティホールや脆弱性は定義されていない。欠陥は売買、保証、瑕疵担保などに定義がある。瑕疵担保の規定はソフトウェアに適用がない。

ただしこの欠陥の定義はウィルスに感染したフロッピーディスクの売買に適用がある(Cass. com., 25 nov. 1997, n.95-14603)。

3.1.3 「セキュリティ・ホール」という用語が法令等で使用されていませんか。

A, ない。

3.2. 責任(Liabilities)

3.2.1 一般的フレームワーク(General frame work)

情報セキュリティ脆弱性もしくは不具合からの責任について、定義や責任が定められていますか。

もし、必要であれば、請求原因を不法行為、制定法、契約法に分けることもかまいません。

民事上の責任について詳細に記述してください。ただし、脆弱性の濫用に対しての刑事的責任および行政的手法についても概観をしてください。

A, 前述の 2.1 を参照。

以下の責任についての論点を考慮にいれて報告ください。

(a) ソフトウエアまたはハードウエアに欠陥があった製造者, 開発者の責任

(b) 「下流責任」(情報セキュリティ侵害攻撃を停止するのに失敗した最初の被害者の責任、すなわち、そのシステムが他者のシステムを攻撃するのに利用された責任-公開されたパッチを宛てるのを怠った責任や公知の脆弱性に対応するのを怠った責任)

(c) システムにおける脆弱性を発見するために効果的な監査を怠った際の責任

A, (a)と(c)は契約責任の事例であり, 前記 2.2.2 参照。実際上は多くが符合契約で免責を定めている。例えば MS WINDOWS2000 参照。

特に(a)については、契約責任を追及できる。ただし、先例はない。

もし物の売買を伴う給付の場合は瑕疵担保責任も問題となる。

2.1.1 で引用した判例では、雑誌付録のディスクがウィルスに感染していたという事例で、購入者が民事責任を追及して認容された。その事件において雑誌編集者は、自らも被害者であること、購入者自身もウィルス防止措置を怠るという過失があったことを主張し、責任を免れようとしたが、控訴院も破毀院もこの主張を認めず、編集者はウィルス防止ソフトを開発するなど、十分な能力があり、ウィルス感染は同社にとって不可抗力とはいえないとした。

(c)については、特約がない限り、手段債務のケースであり、過失の立証を要する。完全な免責規定は判例によれば無効とされている。

(b)について、刑法 226-17 条に基づく責任は認められない。個人情報が漏れたという場合であれば、情報主体は提訴できる。ただし、詐害意図の立証は困難。

3.2.2：**セキュリティ法的責任の要素**(Elements of security legal liability)

情報セキュリティ、機密性、正確性、可用性と法的責任には、どのような関係がありますか。

A. 秘密性および完全性の喪失は、個人情報セキュリティに対する侵害の要件となっている(刑法 226-17 条およびディレクティブ 95/46 号 17 条)。

処分可能性に対する侵害はセキュリティ義務に関する法文の要件ではないが、コンピュータ詐欺の要件と

なる（刑法 323-2 条参照）。

3.2.3 主体的側面(Subjective aspect)

情報セキュリティに対する侵害があった場合に、被害者から責任を追求され得る当事者についてあげて下さい。
具体的に以下の例について記述して下さい。

o ハッカー(脆弱性に対して攻撃するソフトウエアを開発し、意識的に配布するもの)
A．ハッカーの刑事責任はコンピュータ詐欺によって追及されうる。

o 脆弱性の存在するハードウエアまたはソフトウエアの製造業者または開発者
A．3.2.1 参照。

o コンサルタント、システムインテグレーター、配布者、販売業者、その他脆弱性有る技術を推奨したベンダー
o セキュリティの評価やセキュリティ脆弱性の回避を委任されたコンサルタント
A．契約責任が追及されうる（2.2.2 参照）。ただし、それらの者の負う義務は手段債務と評価される。

o 脆弱性を発見する監査人
A．契約責任が追及されうる（3.2.1 参照）。

o 攻撃を抑止するように依頼していたセキュリティ・プロバイダー
A．監査人と同様に、特約をもって特定の結果を約束していれば、契約責任が追及されうる。

o アプリケーションを最新に、パッチを宛ててもらうことにしているアプリケーション・サービスプロバイダー
A．特約をもって特定の結果を約束していれば、厳格な契約責任が追及されうる。

o システムをアウトソースしている場合のホスティング会社
A．特約をもって特定の結果を約束していれば、契約責任が追及されうる。
個人情報が侵害された場合には、当該の情報主体が民事・刑事の責任追及をなしうる。

o 攻撃を許容し、または、停止し得なかった ISP
A．（攻撃を許容していた場合は質問に含まれていなかった）
特約をもって特定の結果を約束していれば、契約責任が追及されうる。
個人情報が侵害された場合には、当該の情報主体が民事・刑事の責任追及をなしうる。

o 脆弱性を発見していながら、それを被害者、ベンダーまたは公に報告しなかった者
A．契約責任又は不法行為責任が考えられる。
電子コミュニケーション分野における個人情報処理およびプライバシー保護に関する 2002 年 7 月 12 日ディレクティブ 2002/58 号は、ネットワークセキュリティ侵害に関する具体的な危険がある場合、公衆がアクセスできる電子コミュニケーションサービスのプロバイダはそのことを会員に伝えるものと定めている（2.1.2 参照）。ただし未だフランス法には移植されておらず、適用されない。

3.2.4 脆弱性の場所

以下のような脆弱性の発生個所によって、責任を問われる人が異なりますか？
- クライアント側
- サーバ側
- ネットワーク機器部分
- など

A. この点についてはフランス法上、立法判例とも存在しない。

以下のようなソフトウエアの提供形態によって、責任の違いを区別しているかを解説してください。
- パッケージ品ソフトウエア（市販品）
- 個別開発品ソフトウエア
- 外注（成果物検収 Deliverable）
- 委託（工数検収 Labor hour）
- サービス提供に利用しているソフトウエア
- など

A. ソフトの供給に関する責任は契約責任であり、従って責任範囲を決めるのは契約条項であって状況ではない。

ただし、パッケージソフトの場合、その約款の有効性は問題となりうるが、判例はまだない。

3.2.5 注意義務-標準(Duty of care-standard)

3.2.5.1 一般(general)

法によって情報セキュリティの基準が定義されていますか。

A. この問題については法令判例とも存在しない。ただし、個人情報がセキュリティの欠陥の修復なしに アクセス可能とされている場合、おそらく、刑法226-17 条の定義するセキュリティ義務違反となるであろう。

脆弱性の改善義務についての基準を法令等で設けているか？

A. 現在のところ法令では存在しない。

法令等以外の情報も知っていれば教えてください。

A. セキュリティについてではないが、ソフトの製品機能と文書に関するISO 15408 が存在する。

CLUSIF (Club de la Sécurité des Systèmes d'Information Français)<http://www.clusif.asso.fr/>は、情報システムセキュリティに関する公益団体だが、情報システムセキュリティ職業規範およびコンピュータセキュリティの職業倫理規範を定めている。ただし、そこにはソフトのセキュリティ不完全を修復すべき義務が書かれているわけではない。

3.2.5.2. 管理者の義務 (Duties of administrators)

システム管理者が、不具合を修正するためになすパッチやソフトウエアを使用することを怠った場合、責任があるか。

A. 特約をもって特定の結果を約束していれば、契約責任が追及されうる。この場合は結果債務となる。
ただし、判例はない。
個人情報が漏洩した場合は刑事責任も追及される。

システム管理者がセキュリティ情報を収集するのを怠ったとき、責任があるか。

A. セキュリティ情報を収集する義務というのはこれまでのものよりも曖昧である。契約上手段債務として責任を負うことはあり得る。

3.2.5.3 インシデントにおけるシステム管理者の義務（Duties of system administrators in case of incidents）
インシデントに対応する際、システム管理者は、不十分な対応しかできなかった場合、または、対応がおくれた場合、責任を負うか。
損害を回避する責任を負う当事者が他にいますか。

A. 契約条項による。

3.2.5.4. セキュリティ・ポリシー(Security policies)

1 注意義務の標準として、セキュリティポリシーを必要としていますか。

A. 例えば、ディレクティブ 95/46 号 17 条は「適切な組織作り」を指示している。
コンピュータセキュリティの一般的な措置に関するCNIL の勧告 81-094 号は、セキュリティ確保のための処置を要求している。
産業医組合の組合長がセキュリティ義務違反で有罪となったのは、訓練を怠ってセキュリティ確保を怠ったためとされる。

2 保険会社や産業界の事業者協会で、ガイドラインを標準としていることはないですか。

A. 3.2.5.1 の回答を参照。

3 セキュリティポリシーの実際の運用が責任に対する抗弁になりますか。
セキュリティポリシーの実際の運用が連邦ガイドラインのようにコンプライアンスの観点から考えられていますか。

A. 責任はケースバイケースで判断される。セキュリティポリシーの実施は評価要素の一つとなる。しかしセーフハーバーというような自動的な免責事由とはならない。

4 セキュリティ上の脆弱性が、セキュリティの監査および評価をしていながら、それを探知できなかった場合、その監査および評価をしていた事実は、抗弁となりえますか。

A. 私見によれば、重要な免責事由となりうる。特に刑事においては。ただし、セーフハーバーというような自動的な免責事由と はならない。

3.2.6 その他（Miscellaneous）
1 セキュリティ・インシデントの実体を明らかにするのに有効だと考えられる法的システムはありますか

A （回答は得られず）

2 「内部告発者保護」や「司法取引」の法制度を有していますか。

A. 密告について規定があるのはテロリズム、麻薬取引についてであり、コンピュータセキュリティについては存在しない。 その他の免責事由もコンピュータセキュリティには関係しない。

司法取引もフランス法には存在しない。現在議会に司法取引を導入する法案が提案されている。

さらに、有罪者の先行出頭と呼ばれる手続の創設が予定されているが、これは司法取引に着想を得たものである。この手続が成立すれば、共和国検事と有罪申告者との取引による刑が、裁判抜きで、裁判所の認可を条件として決定できる。

3 「内部告発者保護」や「司法取引」の法制度が、セキュリティ・インシデントの実体を明らかにするのに有効と考えられるのではないかという議論はありませんか。

A. ない。

3.3 責任ある開示の問題（Responsible disclosure issue）

1．脆弱性に気がついたとき、気がついた人間は、会社や公的機関に報告すべき義務がありますか
2．報告された会社などは、これに対して対応すべき義務はありますか。また、対応をなしうる体制をとっておく義務があると解されていますか。

A. いずれもない。

3．産業界や政府の機関が、脆弱性がわかった際に、それに対して責任有る開示となるようなガイドラインを準備していますか。もし、準備している際は、その内容をお教えください。（

A. ない。

4．脆弱性の報告について、その内容を分析する専門的な委員などの制度が提案されていませんか。もし、議論されているのであれば、その内容をお教えください。

A. ない。

3.4 SQL Slammer の事件をきっかけに何か動きなどがありましたか？

A. ない。

3.5 「ソフトウエアの脆弱性に対応するガイドライン」の観点でご意見があれば教えてください。

A (回答は得られず)

結論

フランス法では、個人情報保護義務について厳格な刑事規制をもっているが、セキュリティについては刑事政策が存在せず、判例もない。しかしながら、将来は発展する分野であろう。

コンピュータセキュリティはむしろ、刑事政策上、コンピュータ海賊に対する追及の角度から扱われている。

『セキュリティホールに関する法律の諸外国調査』報告書

付録　Ｂ－４

英国　報告書日本語訳

（余白）

情報・セキュリティに関する責任についての調査票
経済産業省に対する連合王国[1]に関する応答

バード・アンド・バード、事務弁護士、ロンドン・イングランド

序

この調査のいろいろな点で、より詳細な情報については Encyclopedia of Information Technology Law を参照するように言及する。これは、英国の Sweet & Maxwell 社から発行されているルーズリーフ形式の著作である。バード＆バード事務所の Graham Smith は、Encyclopedia の第７章を記述し、契約によらない責任について触れている。これは、調査票においてカバーされる民事上の責任問題の多くについての詳細な議論を含むものである。

3.1　定義（Definition）

我々は、コンピュータ・セキュリティの欠陥による責任を課す目的のために、『ソフトウェア』、『セキュリティ・ホール』または『脆弱さ』を定義する法規を、知るものではない。『欠陥』という術語は、消費者保護法 1987 において、不完全な製品のための厳格責任を課す目的で、法令での定義を有している（下記で議論する）。

3.2　責任（Liabilities）

3.2.1　一般的なフレームワーク（General framework）

セキュリティ脆弱性または欠陥に対する刑事的な責任（Criminal liability for security vulnerabilities or defects）

連合王国での刑法は、特定のコンピュータ関連の刑事犯罪に関する限り、犠牲者の過失よりむしろ侵入者の行為に注目する。コンピュータ不正使用法 1990 は、コンピュータ・システムへの無権限アクセスに対して、深刻さの程度に応じた 3 つの犯罪を創設した。コンピュータ・システムを無権限アクセスから防御することができなかったことは、何ら犯罪とはされない。そして、不正使用法も（または、他のどの法規も）、コンピュータ・システムが欠陥を有しないことを確保することを怠ったことについて過失があるとしても、コンピュータ固有の犯罪を作るものではない。

しかし、刑事責任は、以下の状況において生じうる。

データ保護（Data protection）

英国では、データ保護法 1998 は EC 指令 95/46/EC（データ保護指令）を実装する。法は、個人のデータが処理される場合に関連する。データ保護原則 7 は、以下のように述べる、

[1] 種々の面で、連合王国における法は、連合王国の構成部分によって異なりうる。特にスコットランドの法は、連合王国の残りと異なる。この調査において、イングランドおよびウェールズの法を叙述した。スコットランドや来たアイルランドにおける差異を叙述するには、さらなる調査が必要である。

「個人データの無権限または違法な処理に対して、偶然の損失または破壊に対して、あるいは、個人データへの損害に対して、適当な技術的かつ組織的措置が採られなければならない」

この原則は、次のように解釈されることを要求される、

「措置を実装するための技術的発展の状態とコストを顧慮するとき､以下の点から適切なセキュリティのレベルを確実にする措置でなければならない

(a) 第 7 の原則において言及される個人データの無権限または違法な処理に対して、そして、偶然の損失または破壊に対して、あるいは、個人データへの損害から、引き起こされうる損害、及び

(b) 保護されているデータの性質。

データ管理者は､個人データにアクセスする従業員すべての信頼性を確実にするために合理的処置をとらなければならない。

個人データの処理が、データ管理者のために、データ処理者で行われる際には、データ管理者は、第 7 の原則に適合するために、

(a) 実行されるべき処理を支配する技術的および組織的セキュリティ措置の観点から、十分な保証を提供する処理装置を選ばなくてはならない、そして、

(b) それらの措置において遵守を確実にするために、合理的なステップを採用しなければならない。

個人データの処理が、データ管理者のために、データ処理者で行われる際には、データ管理者は、以下でないかぎり、第 7 の原則に適合するものとはされない。

(a) 処理は、
(i) 書面により、作成されるか、または、証拠化される、そして、
(ii) データ処理者がデータ管理者からの指示だけに従って行動することになっている、
契約中で行われること、
そして、

(b)第 7 の原則によってデータ管理者に対して課せられるのと同等の義務に応ずることを、データ処理者に対して要求する契約であること」

データ保護原則違反は、それ自体、刑事的責任を惹起するというものではない。しかし、情報コミッショナーが、強制履行通知を送達した際に、強制履行通知に対する懈怠は、（控訴の権利と相当の注意義務の抗弁が存在するとしても）罰金によって罰すべき罪である。

一般の製品・機材の安全性規制（General product and equipment safety legislation）

多種多様な制定法は、建物、器材と製品に安全性の必要条件を課す。これらは、刑事罰で、しばしば裏付けられる。

そのような法規は、コンピュータ装置またはソフトウェアに言及しうるものではないものの、ソフ

トウェア欠陥（たとえばファームウェアまたは埋め込まれたソフトウェアでは）が、ソフトウェアを含んでいる有形的な製品または器材が安全性を欠く場合に適用することができた。これは、安全でない製品または器材に対して刑事罰を問うことがありえた。

そのような犯罪の責任を定めている法律の例は、消費者保護法（Consumer Protection Act）1987（10 条）と一般的な製品安全性規則（General Product Safety Regulations）1994 である。法においては、消費財や仕事場において使われる商品に、一般的な安全性の必要条件に応じる点について過失のあった場合、最高￡5,000 の罰金や 6 月の禁固刑の結果になる。規則の下、消費財に一般的な安全に関する必要条件の不履行があった場合は、￡5,000 までの罰金や最高 3 ヵ月の禁固刑の結果になることがありえる。

消費者に対するサービスの安全は、仕事場の健康と安全性の法律下で取り上げられる。

商品やサービスの安全性に関して、法令によるコントロールについて更に情報（特定セクターにおけるコントロールを含む）を求める場合には、通商産業省ウェブサイト www.dti.gov.uk/ccp/topics1/safety.htm を参照しなさい。

部門的立法（Sectoral legislation）

多くのビジネス部門は、法令の規制を受けており、許認可が必要となることもある。例えば、投資情報サービス、公共医療と電気通信がそのなかに含まれる。そのような産業の規制機関は、情報セキュリティに重点を置いた、そして、そのビジネス・セクターに固有な手順によって実施されうる必要条件を定めうる。

サイバー犯罪条約（Cybercrime Convention）

連合王国は、サイバー犯罪条約に署名したが、いまだ批准していない。

*セキュリティ脆弱性または欠陥に対する民事責任（**Civil liability for security vulnerabilities or defects**）*

不完全なソフトウェアに対する民事責任は、非契約の責任に関しては、連合王国において、裁判所では、いまだ議論されていない問題領域である。この話題の議論は、したがって、他の分野における責任に対するアプローチとの類似によって論ずることとなり、思索的なものになる。

一般に責任が起きうる項目は、

- 契約
- 過失（欠陥を警告する義務の可能性を含む）
- 消費者保護法 1987 の下の不完全な製品に対する厳格責任

そのうえ、ウイルスの拡散については、
- 侵入（トレスパス）
- 迷惑（ニューサンス）

がある。

契約法（Contract law）

契約における用語において明示されるにせよ、黙示の結果にせよ、ソフトウェア欠陥に関する義務が、契約法により発生することがある。契約外の関係者に対して義務を負うことがある。状況によっては、第三者の利益になる契約が結ばれた際に、第三者が、利益に関する義務が不履行になった際には、請求をなすことができる（1999 年契約法（第三者の権利））。

ソフト製品の供給元が、製品で提供されるセキュリティの程度について契約上の約束をするかどうかは、契約条件の問題であり、供給元とその顧客との間の契約の交渉において決まるものである。

非契約責任（Non-contractual liability）

検討中の非契約責任のタイプがなんであれ、有形的損害または人身被害と他の純粋な経済損失の間の区別は、重要である。通常、人身被害または有形資産への損害が予見できる危険性のある場合は、損害が純粋な経済損失である場合に比して、規則は、はるかに広い義務を負わせている。

ソフトウェアの分野では、（たとえば）ウイルスが、有形的損害を引き起こすのか、単なる経済損失だけを引き起こすのかを決定することは、必ずしも簡単であるわけではない。ウイルスが、有形的損害を惹起すると認識されるならば、ウイルスの拡散に関する法律上の注意義務は、単に経済損失だけを引き起こす場合よりも、影響を受ける人に対して、より広範囲な種類の義務を負うとされそうである。

過失（Negligence）

作為にせよ不作為にせよ、他人への損害を引き起こす場合に、責任を負わせるルートは、過失である。何人かが、過失により責任があるとされるためには、以下のことが証明されなければならない。

1.問題の損害を惹起することを回避しうる合理的な注意をなす注意義務を負っていたこと
2.作為または不作為が、必要とされる標準に達しなかったこと
3.作為または不作為が、他の人へ損害を引き起こしたこと
4.損害が、回復するのに遠い原因によるものでは、ないこと

注意義務を負わないかぎり、責任があることはありえない。注意義務を負うかどうかについては、裁判所は、新しい状況において、責任の確立したカテゴリーの類推によって判断し、以下の点を考慮する。

1.当事者の関係は、十分に近接しているかどうか
2.被告が、被った種類の損害を被ると合理的に予見できたかどうか
3.注意義務を負わせることが、公平、適正で合理的かどうか

過失責任について、2 つの主な限界がある。第１の限界は、不完全な製品に対する責任から発生する。1932 年のリーディングケースである *Donoghue v. Stevenson* [1932] A.C. 562 (HL)において、貴族院は、始めて、身体的な被害を引き起こした不完全な製品のメーカーに対して、エンドユーザーへの直接的な責任を課した。この責任は、製品の一度限りの欠陥、デザイン上の欠陥、または、危険物に対する不正確な表示などのような行為や過失から直接に発生するものである。
非常に広い範囲の人に対して、この注意義務を負う。実際、製品の欠陥によって、損害を被ると予測しうる者に対して負うのである。

これらの責任原則は、人身被害および有形的資産への損害への両方に適用される。しかし、*Donoghue v. Stevenson*原則の下で、裁判官は、製品の欠陥が、有形的な、もしくは、人身上の損害を一切引き

起こさなかった場合に、例えば、財政的な損失のような経済的損失のみを回復するのを許そうとはしてこなかった。請求者は、不完全な製品の損失自体を回復することができない。経済損失（例えば利益の損失）は、それが人身被害か有形的な損害の結果として起こる場合にのみ、回復されうる。

過失責任の第２の要素は、情報とアドバイスに対する責任に関する。上述のように、裁判所は、人身被害や有形資産への損害を引き起こしている欠陥製品に関する注意義務を、広範囲に負わせるつもりである。しかし、誤った情報の場合、立場は非常に異なる。人が誤った情報を頼りとして、その結果として、損害を被った場合、裁判所は、（製造物責任ケースとは違って）公平で、当然で合理的である場合には、純粋な経済損失を回復させるつもりであった。

しかし、それは、比較的狭い範囲の人に対して注意義務を負うのとバランスがとれている。裁判所は、情報が信頼されることに関して、広範囲の世界の人々に対して注意義務を負うとすることを極端に嫌がった。注意義務が適用されなければならない情報の提供者と十分に近い関係がある名の知られた人の狭い範囲の人だけに対して、責任を負わせる傾向があった。この種の責任は、*Hedley Byrne & Co Ltd v. Heller & Partners Ltd* [1964] A.C. 465 (HL)において確立された。

情報セキュリティの欠陥が、必ずしも潜在的過失責任のどちらかのカテゴリーに、該当しうると予想できうるわけでない。どんな特定のケースでも、責任は、ソフトウェアのタイプと欠陥の結果に依存しうる。種々のタイプの不完全なソフトウェアに適用しうる過失責任の詳細な議論については、*Encyclopedia of Information Technology Law*（7.18 から 7.43）を参照のこと。

一般的に、欠陥が有形的損害を引き起こしたことをより確信させればさせるほど、裁判所は、損失を被った幅広い範囲の人に対して注意義務を負うようになるといいうる。裁判官が、損失を、基本的に経済的なものとみなす場合には、責任を課するに際して、とても用心深くなっているだろう。

欠陥を警告する義務（Duty to warn of defects）

過失の一般的なカテゴリーの範囲として、我々はまた、既知の欠陥について、メーカーは、警告する法律上の義務を負うこととなるかどうかの問題に言及しなければならない。若干の状況において、裁判所は、販売後においても、そのような義務を製造業者に課すものとしていた。これは、欠陥が人身被害を引き起こした際に、一般の安全関連の事案において起こった。（*Encyclopedia of Information Technology Law*, Chapter 7 paragraphs 7.36 to 7.38 and 7.72 to 7.75 参照）

注文制のコンピュータ・プロジェクトの文脈において、製造業者は、スクリーン上の数字が正確なものとして信頼できなかったと警告することを怠った際には、相当な注意義務が明示されている契約上の債務不履行になると考えられた。過失において、たとえ類似した義務が課されるとしても、幅広い範囲の人に対して負うというよりも、供給元の顧客に対して負う義務となろう。

欠陥の結果が安全問題を含まず、そして、予見できる損害が、純粋に経済的であるか、安全要素を含んでいない有形的な損害の場合に、既知の欠陥を、幅広い範囲の人に対して、警告する義務を負うかどうかは、未決問題のままである。

消費者保護法 1987 の下における欠陥商品に対する厳格責任（Strict liability for defective products under the Consumer Protection Act 1987.）

消費者保護法 1987 は、EU 製造物責任指令（85/374/EEC と 1999/34/EC）を実装した。製造者は、注意義務または過失の存在が証明される必要なしで（￡275 以上高価な）個人財産、生命、人身

の損害を引き起こす製品の欠陥に対して責任がある。
製品の安全性が、人が、一般に備えていると期待するものでなければ、製品は欠陥である。この法律の目的のために、ソフトウェアが製品といえるかどうかという範囲は、明らかではない。この問題の完全な議論は、 *Encyclopedia of Information Technology Law* Chap 7, paras 7.132 to 7.134 でなされている。しかし、この種の責任は、安全性の関連する事例だけに関連するとされている。

*ウイルスの拡散（**Virus dissemination**）*

過失（Negligence）

過失について、上で示したように事案が、有形的な損害または人身被害の予見できる危険性を含む際には、周囲に対して最大に注意する義務の存在を証明することは、一般により簡単である。悪意のあるウイルスが、影響を受けるコンピュータに対して予見可能な有形的な損害を引き起こすかは、議論がありうる（参照*R v Whiteley* [1993] F.S.R. 168, C.A.)。

有形的損害の予見可能性については、ウイルスは、まさしくその目的が、拡散し、有形的な損害を引き起こすことであるから、予見可能性の要素は満たされるように見える。全ての種類の人たち（たとえば、民間の個人を含むこと）に対して、注意義務を負わせることは「公平で、適正で、合理的か」どうかという問題は、裁判所による慎重な考慮を必要とする。

ウイルスの配布に対する過失責任の有無を判断するのにおける難問は、被告に期待される注意義務の標準である。電子ファイルを取り扱う誰でも、渡す前にファイルと電子メールをウイルスチェックすることによって予防措置をとることになっているか？あるいは、例えば、彼らが、ウイルスが、存在するとか本当に存在する危険性があるとかを知っているか、知っていなければならなかったかの時だけ、そうしなければならないのか？同じ標準は、誰にでも適用されるか？または、ソフトウェア出版者、IT プロ、実業家と民間の個人（注意義務を負うと仮定して）は、注意義務について異なった基準を有すると考えられなければならないか？これらの質問は、答えられないままである。

消費者契約法 1987 の下の厳格責任(Strict liability under the Consumer Protection Act 1987)

1987 法の下の責任は、製品に欠陥があると示される場合にのみ起こりうる。ウイルスを含むソフトウェアから成り立つ製品が、頒布された場合に、責任問題が惹起される。しかし、上述のように、ウイルスを含むことが安全性の問題を提起するときのみ、関連性があるだけであった。

Rylands v. Fletcher 原則のもとでの厳格責任 (Strict liability under the rule in Rylands v. Fletcher)

Rylands v. Fletcher 原則（今日では、周りから離れた排出溝に適用されうるニューサンスの法の一種と考えられる）のもとで、本質的に危険なものを土地に運んでおいて、それが、結局、コントロールの効かない他人の土地に排出され、損害を引き起こした場合に、その予見可能である損害に対して厳格責任が課されることになる。

関連するタイプの損害が予見できる限り、有形的な損害の結果として生じる経済損失に損害賠償が原則として及んではならないというのは、理由がないと考えられるけれども、純粋な経済損失は、あまりに遠いものと認識されうる。

-危険な資料の蓄積(Accumulation of dangerous material)

土地に危険物を蓄える者に対して、準則のもと、責任が課せられる。この準則の適用があるとされる従来のカテゴリーの人々についての考え方が、ウイルス撃退ソフトのメーカーまたはコンピュータ・ウイルスのコレクションを管理している大学のコンピューターサイエンス学部について、正確に類推される。

しかし、大部分の人々は、コンピュータ・ウイルスのコレクションを管理し始めない。彼らのシステムは偶然に感染し、そして、偶然、または過失によって、ウイルスを他人に送付してしまう。

-第三者の行為(Third party acts)

原則は、第三者の予見できない行為を通して、危険なものが土地に持ってこられ、排出が起こった際には、被告には責任がないとする。しかし、彼自身過失が、あるならば、責任がありうる。火事の場合、人は、自身の財産に対する火事が第三者によって始まるならば、自身の財産から延焼する火事によって家が破壊されてしまった隣人に対して責任を負うものではない。しかし、不注意にも火の広がりを防ぐことができなかったならば、責任があるようになる。

この推論は、コンピュータ・システムが、第三者の行為のためにウイルスに感染したとしても、合理的な注意を果たせば更なる拡散を防ぐことができたならば、ウイルスのさらなる感染に対して責任がありうるかもしれないことを示唆する。

-土地の自然利用(Natural use of land)

例外が、どの範囲に適用されるかについては、かなり不確実なものであるが、問題の土地が「自然に利用」されていたのであれば、*Rylands v. Fletcher* の原則は、適用されない。上院は、*Rickards v. Lothian* において、「自然利用」に関連し、もし「他人に対する危険を増加するような特別の使い方をなした」場合にのみ原則が適用されるものであり、「単なる通常の使い方とか、共同体の一般の利益になる適切な利用」の際には、適用されてはならないという意味と解釈している。

侵入における責任（Liability in trespass）

状況によっては、商品への侵入の不法行為の理論は、コンピュータ・ウイルスによって財産が損害を受けた者に対する救済の法理として役にたちうる。商品への侵入とは、押収または除去によって、または、商品に対し直接、損害を与えることによってなす商品の所有に対する違法な妨害行為をいう。

上述した *R v. Whiteley* の論理によれば、コンピュータ・ディスクのデータに対するウイルスによる損害は、商品への侵入目的のための損害を構成するように思える。

侵入の不法行為は、故意になす行為（例えば、荒野に故意にウイルスを放つ人のそれ）を確かに含んでおり、過失によってなす行為をも含みうる。しかし、被告の行為に過失が存在しないならば、責任は、存在しえない。

情報技術のシナリオに対する侵入の法理の適用は、英国では、判例法が発展し続けている米国に比して、はるかに発展していない。

3.2.2　セキュリティに対する法的責任の要素（Elements of security legal liability）

上述の議論を参照のこと

3.2.3 主体的側面（Subjective aspect）

- ハッカー（脆弱性に対して攻撃するソフトウェアを開発し、意識的に配布するもの）

コンピュータ・システムへの無権限アクセスをなすようにできているソフトウェア（例えばウイルス）を作成して、配信する人々は、コンピュータ不正使用法 1990 において、罪を犯したとして起訴される可能性がある。ソフトウェアが、システムにおける脆弱性を利用するという事実は、問題に影響を及ぼさない。これは、世帯主がドアをロックすることを怠ったとしても、誰かが中に入ったり家の中身を破壊したりする権利を与えるものではないのと同様である。

そのような人に対しては、少なくとも、被害者が、ソフトウェアが、システムへの有形的な損害を引き起こしたと示すことができるならば、民事訴訟の可能性がありそうである。

- 脆弱性の存在するハードウエアまたはソフトウェアの製造業者または開発者

上で議論したように、原告に対するメーカーまたは開発者の責任は、エンドユーザーとの直接の契約か、メーカーと契約の連鎖を経ての（卸売業者もしくは小売業者を通しての）エンドユーザーとの契約かで管理されるだろう。不法行為（欠陥自体による、または欠陥の警告の不履行によるものどちらでも）におけるエンドユーザーへの直接的な責任がありうるかは、未解決の問題であるが、おそらく、ありそうもない。但し、安全性の要素がある場合は、この限りではない。裁判所は、商業契約の連鎖が存在する際に、経済損失を填補する不法行為の責任（契約論を迂回してしまうことになる）をつくることには躊躇するであろう。

- コンサルタント、システムインテグレーター、配布者、販売業者、その他脆弱性有る技術を推奨したベンダー

原告に対するすべての当事者の責任は、再び、契約で定められるであろう。供給者とコンサルタントの立場について、区別をすることは有用かもしれない。通常、供給者は、その顧客に対して、なんら助言について義務を負わない。満足な品質の、そして、顧客の明示または、黙示による特定の目的に適する（但し、購入者が、販売者の技量や判断に依頼しない、または、依頼することが合理的でない場合は、この限りではない）製品を供給する責任を（契約によって変更されていない限り）負うのである。

供給者と顧客の関係が、十分に密接であるならば、助言する（そして、警告する）義務が、不法行為において、認められうる。そのため、供給者は、実際、コンサルティングの役割を引き受ける。パッケージ・ソフトの供給者の責任は、特別な状況である。（*Encyclopedia of Information Technology Law* Chap 7, paras 7.60 to 7.71.）

- セキュリティの評価やセキュリティ脆弱性の回避を委任されたコンサルタント

コンサルタントは、通常アドバイスをする際にクライアントに対する合理的注意を働かせる義務を有するが、通常、アドバイスの結果を請け負わ（例えば、保証し）ない。おそらく安全性の過失の場合以外には、クライアント以外の者に対して義務があるということは、ほとんどありそうもない。

- 脆弱性を発見する監査人

監査役が、責任があるどうかは、とりわけ、その権限の範囲に依存する。どんなプロのアドバイザーと同様にでも、監査役は通常アドバイスをする際にクライアントに対する合理的注意を働かせる義務を有するが、通常、アドバイスの結果を請け負わ（例えば、保証）ない。監査役が、監査役のレポートに依拠した場合に、クライアント以外の者に対する義務がありうる範囲に関して、かなりの判例法がある。これは、レポートの内容に対して、監査役が責任を引き受けたとされる密接な周囲の人々のグループを越えて、裁判官が、義務を負う人を広げるのに気が進まない状況の古典的な例である。

- 攻撃を抑止するように依頼していたセキュリティ・プロバイダー

セキュリティ・プロバイダーと原告との関係が、明白な契約で定められることは、ほとんど間違いがない。安全性の過失以外に、顧客以外の者に対して義務を負うということは、ほとんどありそうもない。

- アプリケーションを最新に、パッチを宛ててもらうことにしているアプリケーション・サービスプロバイダー

アプリケーション・サービスプロバイダと原告の関係が、明白な契約で定めることはほとんど間違いがない。安全性の過失以外に、顧客以外の者に対して義務を負うということは、ほとんどありそうもない。

- システムをアウトソースしている場合のホスティング会社

ホスティング会社と原告との関係が、明白な契約で定められることは、ほとんど間違いがない。安全性の過失以外に、顧客以外の者に対して義務を負うということは、ほとんどありそうもない。

- 攻撃を許容し、または、停止し得なかった ISP

ISP が、直接、原告のインターネット接続に対して責任があるならば、ISP と原告の関係が、明白な契約で定められることは、ほとんど間違いがない。そうでない場合には（すなわち、ISP が上流の場合）、世間の人々に対して法が責任を課す状況について上述の一般的な分析が参考になる。原告が、純粋な経済損失を被ったと認識される場合、ISP が、世間一般にたいして注意義務を負うことは、もっともありそうもない。有体的損害または人身被害が予見できるならば、状況は異なるかもしれない。

たとえ注意義務が存すると判断しても、因果関係を証明することは、きわめて困難でありうる。損害を被った原告にしてみれば、どの ISP、ネットワーク、接続プロバイダでも、ワームが通ったシステムは、同様に攻撃が通過するのを許容したに違いない。

何を根拠として、原告は、プロバイダーを見つけて、その特定のプロバイダーの過失が損害を引き起こしたと主張することができるか？　これは、困難な問題を提起する。裁判所は、1 つの ISP（おそらく最初のもの）の過失が支配的な原因であったと判断するかもしれない。また、2 つ以上が、共同で損害を引き起こしたと判断するかもしれない。

- 脆弱性を発見していながら、それを被害者、ベンダーまたは公に報告しなかった者

ベンダーが警告を懈怠していたことに対する責任については、上述の議論を参照のこと。安全性の欠陥を含んでいる特別の状況は格別として、そうでない場合において、我々は、当事者が、警告する注意義務がある部類に入るかどうか疑問に思う。

3.2.4　脆弱性の場所（Location of vulnerability）

我々は、脆弱性の場所に関して、一般的なルールが有効に定まっているとは、確信していない。関連した器材やそこで使用されるソフトウェアの責任は、場所（場所がどの国の法律を適用するかについて決定することに非常に関連するかもしれない国境を越える事案以外）よりも関連性がある。

ソフトウェアを提供する方法（パッケージ、注文制その他）は、存在しうる注意義務の範囲に影響を及ぼすだろう。これは、 *Encyclopedia of Information Technology Law* Chap 7, paras 7.29 to 7.32 において、詳細に議論される。

3.2.5　注意義務（Duty of care - standard）

3.2.5.1　一般論（General）

過失責任における注意義務の標準にについては、*Encyclopedia of Information Technology Law* Chap 7, paras 7.85 to 7.94.参照。

過失において、注意義務の基準を評価するとき、裁判所は、決定的というわけではないが、自主的な業界標準を考慮に入れる。

興味ある源の一部としては、以下のものがある。

- ネットワークと情報・セキュリティにおける一般のアプローチと特定の行動に関する 2002 年 1 月 28 日の EU 会議解決（2002/C 43/02）

- NISCC（国家基盤セキュリティ調整センター）（www.niscc.gov.uk）と UNIRAS（英国政府 CERT）（www.uniras.gov.uk）の出版物

- ISO-17799/BS 7799（情報技術（情報セキュリティ・マネジメントの実務コード））

- ISO-15408（コモン・クライテリア）

- 通商産業省（DTI）出版『The Business Manager's Guide to Information Security（経営者のための情報セキュリティについてのガイド）』。

- 通商産業省（DTI）出版『'The 1998 Data Protection Act. Have you considered using BS 7799?（データ保護法 1998。あなたは、BS 7799 を使うことを考えたか？）』

- National Computing Centre 出版『ISO 17799 に証明されたようになって、情報・セキュリティを管理すること』

管理された産業部門において、セキュリティに関するより特定的な必要条件やガイダンスが、ますます一般的になっている。例えば、

健康

- Department of Health（保健省）出版『'The Protection and Use of Patient Information: Guidance from the Department of Health' (2001)（患者情報の保護と利用－保健省からのガイダンス（2001））

- The Joint Computing Group of the General Practitioners' Committee and the Royal College of General Practitioners（一般開業医委員会と一般開業医ロイヤル・カレッジとの共同コンピューティング・グループ）『Good Practice Guidelines for General Practice - Electronic Patient Records（一般医療（電子患者記録）のための良い実務ガイドライン）』（2000 年 8 月 31 日）

- The National Health Service (General Medical Services) Amendment (No. 4) Regulations 2000（ 国民医療制度改正（一般的な医療）（No.4）規則 2000）。
これらは、医者によって記録がコンピュータによって作成されるための規定を作成し、それらは、「General Medical Practice Computer Systems - Requirements for Accreditation - RFA 99（RFA99－一般医療実務コンピュータシステム承認条件）と医者が、前述の「Good Practice Guidelines」を参照するという約束を含むものである。

電気通信

- 2002 年 10 月 9 日、電気通信会長によって『Guidelines on the essential requirements for network security and integrity and criteria for restriction of access to the network（ネットワーク・セキュリティと完全性のために重要な必要な条件とネットワークへのアクセス制限の基準のガイドライン）』についての声明。ガイドラインと基準付き。これらは、公共電気通信運営者の２０の許可条件に言及し、ネットワーク・セキュリティと完全性に関する必要条件を含む。

-指令 97/66/EC（電気通信データ保護指令）。これは、指令 2002/58/EC（プライバシーと電子通信に関する指令）によって、2003 年 10 月 1 日に取って代わられる。これらの指令の各々は、セキュリティに関して準備を含む。現在の指令は、第 4 条において、

1.
公的に利用可能な電気通信サービスのプロバイダは、必要であるならば他の公的電気通信ネットワークのプロバイダとともにネットワーク・セキュリティに関して、そのサービスのセキュリティを保護するための適当な技術的かつ組織的な措置をとらなければならない。技術水準と実施にかかる費用を顧慮しつつも、これらの措置は、起こりうるリスクにふさわしいセキュリティのレベルを確実にするものでなければならない。

2. ネットワークのセキュリティが破られる特定のリスクがある場合には、公的に利用可能な電気通信サービスのプロバイダーは、そのリスクと可能な救済策について、関係する経費を含んで加入者に知らせなければならない。」

新しい指令は、第 4 条で、
「1.
公的に利用可能な電気通信サービスのプロバイダは、必要であるならば公的電気通信ネットワークのプロバイダとともにネットワーク・セキュリティに関して、そのサービスのセキュリティを保護するための適当な技術的かつ組織的な措置をとらなければならない。技術水準と実施にかかる費用を顧慮しつつも、これらの措置は、起こりうるリスクにふさわしいセキュリティのレベルを確実にするものでなければならない。

2. ネットワークのセキュリティが破られる特定のリスクがある場合には、公的に利用可能な電気通信・サービスのプロバイダーは、そのリスクについて、加入者に知らせなければならず、そのリスクが、サービスプロバイダーによって採られた措置の範囲の外にある場合には、可能な救済策について、かかりそうな経費をも示して加入者に知らせなければならない。」

英国では、既存の指令は、電気通信（データ保護とプライバシー）規則 1999 によって実装される。規則 28 条は、

「電気通信サービスのセキュリティ

28　（1）パラグラフ(2)に従って、電気通信サービスプロバイダは、提供するサービスのセキュリティを確保するために適切な技術的かつ組織的な措置をとらなければならない。

(2) 必要であるならば、パラグラフ(1)によって必要な措置は、この目的のためにサービスプロバイダによってなされる合理的要請に対して応じなければならない関連した電気通信ネットワークのプロバイダとともに、電気通信サービスプロバイダによってとられる。

(3) これによって必要な処置をとることにもかかわらず、関連した電気通信ネットワークのセキュリティに対して重要なリスクがある場合には、電気通信サービスプロバイダは、関係する加入者に

(a) そのリスク

(b)そのリスクに対する予防手段をもつ採用しうる適切な対応措置そして、

(c) そのような措置をとることに関係している経費。

を知らせる

(4) この規則の目的のために、措置は、
(a) 技術的発展の状態、そして、
(b) 処置を実装するためのコスト、
に照らして、適切であるとみなされるだけである

それらは、安全装置で対応すべきリスクと比例している。

(5) [省略]」

規則 35 は、

「規則 35 の要件に対する不履行の補償。
－（1）他者による規則の必要条件違反の理由により損害を被った人は、その損害にたいして補償を受けることができる。

(2) この規則に関し進められる手続きにおいて、必要なすべての状況において関連する必要条件に対応すべく、しかるべき注意をとっていたことは、抗弁となる。」

データ保護法 1998 の下において、情報コミッショナーの執行権力は、また、これらの規則まで広げられる。

英国政府は、新しい指令を実装するために提案された規則について現在、コメント募集中である。

3.2.5.2 管理者の義務（Duties of administrators）

我々は、法律上、そのような義務を管理者に特に置いているいかなる立法も知らない。

3.2.5.3 インシデントに対するシステム管理者の義務（Duties of system administrators in case of incidents）

我々は、法律上、そのような義務を管理者に特に置いているいかなる立法も知らない。

損害の軽減については、ウイルスから被害を被った過失ある当事者（例、既に告知されていたパッチをインストールすることができない場合）は、寄与過失あるものとして、過失相殺をされる危険がある。また、原因者によって提起された損害を軽減する義務があることになろう。

3.2.5.4 セキュリティポリシー（ Security polices）

1.上述の議論参照のこと
2,存在しない。
3,および 4 これは、当事者が、(合理的な注意を払うことが必要条件になっていた場合には)合理的な注意を払っていたかどうかを示すことができたかどうかの問題である。セキュリティポリシーのパフォーマンスは、それを証明する際に、確かに関連する。

3.2.6 その他（Miscellaneous）

1. 英国に、『告発者保護』法がある。これは、公的関心発表法 1998 によって導入された。
2.
我々は、そのような議論については、知らない。
3.

我々はこの質問についてコメントすることができない。そして、それはこの調査の範囲外である異なる法律制度の比較を含むように思われる。.

3.3 責任ある開示の問題（Responsible disclosure issue）

1. **「警告義務」に関する上述の議論参照のこと**
2. **我々は、何も知らない。しかし、**the National High Tech Crime Unit**（国営ハイテク犯罪部門）は、企業が匿名でコンピュータ犯罪を報告できる秘密を維持しうる団体を設けた。**

3.4 SQL Slammer incident

SQL **スラマー事件は、一般にコンピュータ・セキュリティとサイバー犯罪立法についての既存の議論を再び呼び起こした。**

3.5 Codes of conduct regarding software vulnerabilities

上述の section 3.2.5.1 **を参照のこと**

Bird & Bird
90 Fetter Lane
London,
England
EC4A 1JP

+44 (0)20 7415 6000 (t)
+44 (0)20 7415 6111 (f)

Ref: GJHS
25 June 2003

5 ドイツ

ドイツ連邦共和国の回答

3.1 定義
3.1.1. 脆弱性を議論するにあたって、「ソフトウェア」の定義が法にありますか

A2:設問に対して直接該当する法令等は存在しないが、関連するものがある
DIN/ISO 規格 9000、第 3 部の定義(ソフトウェアの開発、提供および保守に対するISO9001 の適用のための便覧(1992 年))は次のように述べている。
「ソフトウェア:情報処理プログラムによる作業に属する、プログラム、プロセスならびにそれに属するすべての仕様書から構成される精神的製品(No. 3.109)
ソフトウェア製品:ユーザに提供するよう決められているコンピュータプログラム、プロセスならびにこれに属する仕様書およびデータ一式全て」

3.1.2. 「セキュリティホール」「脆弱性」「不具合」について法令等で定義をしていますか
A2:設問に対して直接該当する法令等は存在しないが、関連するものがある
「セキュリティホール」「脆弱性」については存在しない。
ただし、「不具合(Fehler)」については、瑕疵担保責任における「瑕疵」の概念が場合によりカバーし、また製造物責任法 3 条の「欠陥(Fehler)」が定義を有している。また、DIN6627 がソフトウェアの不具合についての判断を扱っている。

3.1.3 「セキュリティ・ホール」という用語が法令等で使用されていませんか。
A3-1:設問に対して該当する法令等は存在しない

3.2. 責任
3.2.1 一般的フレームワーク
情報セキュリティ/脆弱性もしくは不具合からの責任について、定義や責任が定められていますか。もし、必要であれば、請求原因を不法行為、制定法、契約法に分けることもかまいません。民事上の責任について詳細に記述してください。ただし、脆弱性の濫用に対しての刑事的責任および行政的手法についても概観をしてください。

以下の責任についての論点を考慮にいれて報告ください。
(a) ソフトウェアまたはハードウエアの欠陥について製造者または開発者の責任(すでに利用されているプログラムの事後的な修正に利用されるパッチ、部分的なプログラムも含む)
ソフトウェアの製造者もしくは開発者は、典型的には、契約に基づいて責任を負う。標準的なソフトウェアを引き渡す場合には、売買契約が問題となり、瑕疵担保責任が問われる。また、不法行為法の製造者責任の諸原則または製造物責任法による責任を考えることになる。

(b) 情報セキュリティに対する攻撃の最初の被害者の責任、すなわちさらなる攻撃を阻止することを懈怠したことが、自己の管理するシステムが他の被害者のシステムに損害を与えることにいたった者の責任（公開されたパッチの適用義務や公知の脆弱性を無防備にしておかない義務を含む）

最初の被害者の刑法上の責任は故意がないために阻却される。過失は処罰規定がない。

民法 823 条 1 項による最初の被害者の不法行為責任は十分ありうる。たとえば、最初の被害者が不十分なセキュリティシステムを理由としてウイルスの拡散、したがってより大きな危険源の放置について責任があるという場合ついて可能である。

(c) システムの脆弱性の効果的なセキュリティ監査を怠ったことについての責任

システムの脆弱性の監査に関する契約が当事者間に存在するかぎり、システムの脆弱性の効果的な監査を明示することを怠った者は、契約に基づき責任を負う。

ハンブルクラント裁判所の2001年7月18日の確定力ある判決 (Aktenzeichen 401 O 63 /00) によると、データメディアをウイルス感染の検査を契約により引受けた会社は、最新でない検査プログラム使用したことによって検査の際にウイルスを見逃した場合に生じた損害について責任を負う。

3.2.2 :セキュリティ法的責任の要素 (Elements of security legal liability)

情報セキュリティ、機密性、正確性、可用性と法的責任には、どのような関係がありますか。

訴訟を起こすかぎり、企業は、その手続の範囲において、その現存のソフトウエアシステムについての機密性のある秘密情報を明らかにすることが必要となる。ただし、重要な取引上もしくは営業上の秘密に関係する場合は、非公開の手続が可能である。

3.2.3 主体的側面

情報セキュリティに対する侵害があった場合に、被害者から責任を追求され得る当事者についてあげて下さい。
具体的に以下の例について記述して下さい。

? ハッカー

攻撃者は、故意に損害を惹起した場合、刑法上の責任がある。さらに、被害者は不法行為による請求を主張することができる。

? 製造者あるいは開発者

典型的には、製造者または開発者は、被害者と締結した契約により責任を負う。そのほかにも、この場合、民法 823 条による製造者責任および製造物責任法による製造物責任が適用されるべきである。

? コンサルタント、システムインテグレーター、配布者、販売業者、あるいは欠陥のある技術を推奨しまたは指図したその他ベンダー（場合によっては、製造物の製造者との内部的な関係における連帯債務による責任）

標準的なソフトウェア販売業者の場合、製造者から発したコンピュータプログラムを故意にウイルスによって感染させないということが前提となる。

販売業者がソフトウェア製造業者によって販売用に完成して引き渡されたパッケージを独自に製造的な作業をせずにさらに販売するという場合がよくある。売主として、販売業者は、顧客に損害が生じないようにする付随的義務を有している。この限度で、故意もしくは過失で行為した（中間）販売業者も、コンピュータウイルスによって惹起された損害について責任を負う。しかしながら、そのような者は、前段階の供給者、たとえばプログラムの製造者に賠償させることができ、支払った損害賠償を求償することができる。

しかも、製造業者を確定することができない場合。製造物責任法 4 条 3 項により、供給者を製造物責任法による製造業者とみなす。このことにより、ユーザは、製造業者がわからないために、自己の請求を達することができないという事態から保護される。

供給者は、当該請求が到達した後一ヶ月以内に被害者に製造者または先行供給者を知らせた場合、以上の代替責任を免れることができる。

OEM 販売業者は、その製造監視義務を遵守しなかった場合、過失により行為している（民法 823 条 1 項）。その限度で、先行供給者、たとえばプログラム製造業者に損害を払わせることはできない。

? セキュリティの脆弱性の評価および回避を委任されたコンサルタント

すでに上記の 3.2.1(c)で説明した、2001 年 7 月 18 日のハンブルクラント裁判所の判決が参考になる。データメディアをウイルス発生について検査することを契約によって引受けた会社は、検査の際に、最新ではない検査プログラムを使用することによってウイルスを見逃した場合、発生した損害について責任を負う。

? インターネットサービスプロバイダ

インターネットサービスプロバイダの場合、通常、プロバイダとコンテンツ提供者との間には記憶領域の提供に関して契約が存在している。サービスプロバイダが用意された他人のコンテンツに関して予防的な監督義務にどの程度服するのか、したがって、ウイルスの発生が存在しないことを一定の事情のもとでもしくは通常確証する義務があるのかどうかが問題となる。

自らのところに蔵置され用意されているコンテンツに関する検査義務は、原則として、サービスプロバイダに課すべきではない。契約の相手方が適法に行動することを前提にすることが許されなければならない。

しかしながら、サービスプロバイダが具体的な法侵害を理由とする指摘あるいはそれどころか警告を受け取った場合は、積極的な認識をもったこの時点から服すべきことになる。この場合、遮断することも技術的に期待可能であるといってよい。テレサービス法 11 条により、プロバイダは、認識がある場合、遅滞なく活動しなければならない。

サービスプロバイダが情報の伝送の誘因となっていないかぎり、テレサービス法 9 条 1 項により刑法、損害賠償法および行政法の各領域での責任はない。これはコンピュータウイルスについても妥当する。

? 脆弱性を認識したが、これを報告しなかった当事者
ある当事者が報告を怠ったことについて責任を負うのは、そのような報告をおこなうことを義務を負っている場合のみである。このような義務は、契約関係の存在または一般的な保証義務のいずれかから導き出すことができる。
後者の義務を認めることができるのは、監督ないし監視義務を引受けていた場合だけであるが、しかし、なんらかの形態での危険源についても責任がある。

3.2.4 脆弱性の提供方法
以下のような脆弱性の発生個所によって、責任を問われる人が異なりますか？
- クライアント側
- サーバ側
- ネットワーク機器部分
原則として、被害の場所は損害賠償義務について重要ではない。もちろん、保護義務の程度は、個々のクライアントにおけるよりもネットワークにおけるほうがより高度となりうる。

以下のようなソフトウェアの提供形態によって、責任の違いを区別しているかを解説してください。
- パッケージ品ソフトウェア（市販品）
- 個別開発品ソフトウェア
  - 外注（成果物検収 Deliverable）
  - 委託（工数検収 Labor hour）
- サービス提供に利用しているソフトウェア
ソフトウェアを提供する態様は契約類型を決める際に重要となる。したがって、どの保証条項が適用可能となるかという問題についても重要な役割を果たす。

3.2.5 注意義務-標準
3.2.5.1 一般
法によって情報セキュリティの基準が定義されていますか。
脆弱性の改善義務についての基準を法令等で設けているか？
法令等以外の情報も知っていれば教えてください。

A1:設問に対して該当する法令等は存在しない。
セキュリティの詳細な基準を法定することは、情報技術の進展にとって有害である。枠組み的なものとして、BSI の「情報技術のシステムのセキュリティ監査に関する基準」がある。その他、関連する法規として連邦データ保護法(BDSG)9 条が個人情報について規定する。なお、契約上

の義務については判例がある。

3.2.5.2. 管理者の義務

システム管理者が、不具合を修正するためになすパッチやソフトウェアを使用することを怠った場合、責任があるか。

システム管理者がセキュリティ情報を収集するのを怠ったとき、責任があるか。

契約上の義務が存在する場合、その違反について責任を負う。義務の内容は契約の類型により異なる。

3.2.5.3 インシデントにおけるシステム管理者の義務

インシデントに対応する際、システム管理者は、不十分な対応しかできなかった場合、または、対応がおくれた場合、責任を負うか。

管理者に故意または過失があるといえるかどうかは、つねに個々の事案における具体的な衡量の問題である。場合により、賠償責任を負うことがあるが、原則としてすでに不法行為ないし義務違反による当事者の責任が生じていることに注意すべきである。

損害を回避する責任を負う当事者が他にいますか。

被害者についても、法律上の損害回避義務が存在する。被害者が損害を軽減する義務を怠った限度で、民法 254 条 2 項が関係することになる。被害者が損害の回避もしくはその軽減に十分な程度に寄与しなかった場合、損害賠償請求はそれに応じて減額される。

判例は、その場合、様々な技術的な可能性（データの保全、ウイルスの検査）と行動準則を遵守しなかった場合、損害が発生したときでも、共同責任があると判断している

3.2.5.4. セキュリティ・ポリシー

1 注意義務の標準として、セキュリティポリシーを必要としていますか。

情報セキュリティにおける注意義務の規準について詳細な法律上の規定は存在しないことから、一般的な責任の規範が独自の具体的なセキュリティポリシーの作成を要求することになる。あらゆる製造業者、開発者、供給者などは、必要な注意義務の規準を充足するために、そのソフトウェアをその技術の現在の基準に適合させるよう義務づける。

2 保険会社や産業界の事業者協会で、ガイドラインを標準としていることはないですか。

BSI が以下のものを公開している。

IT 安全性基準 http://www.bsi.de/zertifiz/itkrit/itkrit.htm
IT 基本保護ハンドブック http://www.bsi.de/gshb/deutsch/menue.htm
その他、http://www.bsi.de/fachtem/sinet/index.htm

なお、ヨーロッパのレベルでは「情報技術セキュリティ評価基準?ITSEC」がある。

3 セキュリティポリシーの実際の運用が責任に対する抗弁になりますか。
枠組みだけでしかなく、具体的な内容は不明確であるため、なりえない。

4 セキュリティ上の脆弱性が、セキュリティの監査および評価をしていながら、それを探知できなかった場合、その監査および評価をしていた事実は、抗弁となりえますか。
一般的な品質基準を維持するかぎり、私法上、有責性を認めるべきではない。一般的なセキュリティ基準が通常アップデートされ、検証されている場合、ウイルスの発症に関して有責性を認めることはできず、そのため責任が阻却される。
周知の方法によって検地されず、したがって阻止することもできなかった新種のウイルスについては、ソフトウェア開発者あるいは製造業者に責任を問うことはできない。
したがって、この局面のもとでは、通常の、かつ技術の最新の基準を維持したセキュリティ監査を実行することは「セーフ・ハーバー」となる。

3.2.6 その他
1 セキュリティ・インシデントの実体を明らかにするのに有効だと考えられる法的システムはありますか。
A2:設問に対して直接該当する法令等はないが、関連するものがある。
この点に関して特別の法令等は存在しない。しかしながら、作為義務は契約または不法行為により生じうる。

2 「内部告発者保護」や「司法取引」の法制度を有していますか。
A2: 設問に対して直接該当する法令等はないが、関連するものがある。
裁判所手続法(GVG)172 条 1a 号や刑事訴訟法 68 条、247 条 a の手続き上の保護がある。
自白により立証されて有罪判決をおこなう場合、刑の減軽は可能である。

3 「内部告発者保護」や「司法取引」の法制度が、セキュリティ・インシデントの実体を明らかにするのに有効と考えられるのではないかという議論はありませんか。
この点に関して議論が見受けられない。

3.3 責任ある開示の問題
脆弱性に気がついたとき、気がついた人間は、会社や公的機関に報告すべき義務がありますか
労働関係がある場合にも、両当事者の、他方の権理、法益および正当な利益を配慮する義務は存在する。特別の付随義務として、従業員は、労働契約および雇用主の指示により概要が示されるその活動範囲において発生しあるいは切迫している損害をともかく雇用主に報告しなければならない。

報告された会社などは、これに対して対応すべき義務はありますか。また、対応をなしうる体制をとっておく義務があると解されていますか。

（回答なし）

産業界や政府の機関が、脆弱性がわかった際に、それに対して責任有る開示となるようなガイドラインを準備していますか。もし、準備している際は、その内容をお教えください。

脆弱性の報告について、その内容を分析する専門的な委員などの制度が提案されていませんか。もし、議論されているのであれば、その内容をお教えください。
A4:不明

3.4　SQL Slammer の事件をきっかけに何か動きなどがありましたか？
　連邦政府のセキュリティ・イニシアティブ、たとえば「安全なインターネット」や「安全なインターネット産業のパートナーシップ」というタスクフォースとならんで、BSI は、今年、インターネットにおけるセキュリティを実行に移す場合にとくに市民を支援することになるイニシアティブをスタートさせた。www.bsi-fuer-buerger.de 参照。

3.5　経済産業省が「ソフトウェアの脆弱性に対応するガイドライン」を作成するとしたら、経済産業省に対して、ご意見・推奨があれば教えてください。
　この点については、回答書の詳細を参照のこと。

6　大韓民国

情報セキュリティ比較調査研究　質問事項に対する回答

（大韓民国　㈱ローアンドビー　代表取締役／弁護士　李　海完）

　下記の質問事項に対する韓国の法規、判例、学説、その他の情報を参考に次のように回答いたします。

III.　質問事項(The Questions)

以下においては、「法」という用語を、この質問票に関するかぎり、制定法、規則、法令、判決例、行政規則などのすべての公の準則をいうものとする。

3.1 定義(Definition)

3.1.1.脆弱性を議論するにあたって、「ソフトウエア」の定義が法にありますか。

　【回答】脆弱性と関連した脈絡に限定されることではないが、「ソフトウェア」の定義を規定した法条文がある。ソフトウェア産業振興法第２条第 1 号において「『ソフトウェア』というのはコンピュータ・通信・自動化などの装備とその周辺装置に対して、命令・制御・入力・処理・保存・出力・相互作用が可能になるようにする指示・命令（音声または映像情報などを含む）の集合と、これを作成するために使用された技術書その他関連資料をいう。」と定義しているのがそれである。これが韓国の法律上ソフトウェアの定義を下している唯一の規定だと判断する。ソフトウェアと類似した概念としてコンピュータプログラムという用語があるが、これに関しては著作権法　第２条第１２号にて「コンピュータプログラム：特定の結果を得るためにコンピュータ等の情報処理能力を持つ装置内で直接または間接的に使用される一連の指示・命令によって表現されたものをいう。」と定義規定をおいてあり、コンピュータプログラム法第２条第１号において、コンピュータプログラム著作物に対して、「『コンピュータプログラム著作物』とは、特定な結果を得るためにコンピュータなど情報処理能力を持つ装置（以下「コンピュータ」という）内で直接または間接に使用される一連の指示・命令で表現された創造物をいう」と定義規定をおいている。著作権法とコンピュータプログラム保護法にて定義されたコンピュータプログラムは、著作権法上、著作物の一つとして取り扱われている脈絡でコンピュータプログラムを定義した規定だ。ここで定義されたコンピュータプログラムの意味をソフトウェア産業振興法によって定義された「ソフトウェア」の意味と比較してみると、ソフトウェアの意味がプログラムに比べて「・・・これ（*プログラム）を作成するために使用された技術書その他関連資料」を含めているという意味で、その分もっと広い概念であることが分かる。

3.1.2.「セキュリティホール」「脆弱性」「不具合」について法令等で定義をしていますか。

【回答】韓国法で法令用語に外国語を直接使用している例が増えているが、原則的には韓国語に換えて表現するよう努力している。そこで、「Security　Hole」も韓国法では「脆弱点」という韓国語に換えて使用している（即ち、韓国法で使用している脆弱点という用語は、「security hole」と同じ意味と判断されている）。ただし、これに対する定義規定を法に定めてはいない。‘脆弱点’という用語を使用している法令は２００１年１月２６日に制定された法律である「情報通信基盤保護法」（２００２年１２月１８日一部改正）とその施行令である（添付資料＃1、＃2参照）。一方、「情報通信網利用促進ならびに情報保護に関する法律」に基づいて情報通信部長官が制定し公示した「情報通信サービス情報保護指針」第８条において「保安脆弱点」という用語を使用しているが、同じような意味の用語であるといえる（添付資料＃８参照）。

情報保護と関連して一般的な事項は、「情報通信網利用促進ならびに情報保護に関する法律」において規定しており、特に国家的・社会的重要性を持つ重要情報通信基盤施設をサイバーテロ攻撃などから保護する問題に対しては、「情報通信基盤保護法」で規定している。

「欠陥」という用語は、「脆弱点」とは多少異なる概念として一般製造物の欠陥で起因した製造物責任と関連して使用される用語で、製造物責任法において、その定義規定をおいてある。即ち、製造物責任法第２条にて、「『欠陥』というのは、該当製造物に次の各目のひとつに該当する製造・設計または表示上の欠陥、もしくは、その他通常、期待できる安全性が欠けているということをいう。」と定義している。

3.1.3.「セキュリティ・ホール」という用語が法令等で使用されていませんか。

【回答】上記の質問に対する回答を参照。

3.2. 責任(Liabilities)

3.2.1　一般的フレームワーク(General frame work)

情報セキュリティ脆弱性もしくは不具合からの責任について、定義や責任が定められていますか。

【回答】特別に対象を限定して、情報セキュリティの脆弱性と関連した責任にまたは、ソフトウェアの欠陥に対する責任に関して特別に民事責任要件等を規定した法令はない。「情報通信網利用促進ならびに情報保護に関する法律」および「情報通信基盤施設保護法」上のいくつか義務規定が、民事責任の一つの要素である過失の有無の判断に対して一つの基準になり得るだけである（このような規定の詳細な内容は、後で該当する質問へ答えながら紹介していく）。結局、民事責任の有無と損害賠償の範囲等を決めるに当たって、民法上の不法行為、債務不履行、製造物責任法上の製造物責任等に該当するか否かを検討することとなる。

もし、必要であれば、請求原因を不法行為、制定法、契約法に分けることもかまいません。

【回答】以下で、民事責任の類型を不法行為、債務不履行、製造物責任など、三つに分けて、一般的フレームワークに関する説明をする。

民事上の責任について詳細に記述してください。ただし、脆弱性の濫用に対しての刑事的責任および行政的手法についても概観をしてください。

【回答】下記では、刑事責任と行政的な事項に対して別途説明をすることとする。

以下の責任についての論点を考慮にいれて報告ください。

(a)　ソフトウェアまたはハードウエアに欠陥があった製造者,開発者の責任
(b)　「下流責任」(情報セキュリティ侵害攻撃を停止するのに失敗した最初の被害者の責任、すなわち、そのシステムが他者のシステムを攻撃するのに利用された責任-公開されたパッチを宛てるのを怠った責任や公知の脆弱性に対応するのを怠った責任)
(c)　システムにおける脆弱性を発見するために効果的な監査を怠った際の責任

【回答】上記の問題に対しても下記で一緒に述べることとする。

【回答】情報セキュリティに関する責任の一般的フレームワーク
１．民事責任

上で回答したように民事上責任を問う請求原因を、不法行為、債務不履行、製造物責任の三つの類型に分けて報告する。

（１）不法行為

韓国で不法行為は、一般不法行為と特殊不法行為に分けられる。一般不法行為とは、不法行為に関する基本的な条項である民法第７５０条（故意または過失による違法行為により他人に損害を与えた者は、その損害を賠償する責任がある）の規定による不法行為をいい、特殊不法行為とは民法第７５０条に対して特則を規定した特別法に基づく不法行為をいう。
自動車損害賠償保障法において、無過失責任に取り扱っている自動車事故などの場合がこれに該当し、後で述べる製造物責任もこれに該当しているといえる。
韓国法上、ＩＴの領域にも不法行為と関連した特則規定が、何箇所かで規定されている。その中の一つが個人情報の侵害に関連して、侵害者の故意、過失に対する立証責任を転換した「情報通信網利用促進ならびに情報保護に関する法律」第３２条の規定［利用者は、情報通信サービス提供者などのこの章の規定に違反した行為により損害を受けた場合には、その情報通信サービス提供者などに対して損害賠償を請求できる。この場合、当該情報通信サービス提供者などは故意または過失がないことを立証しなければ責任を免れることはできない。］であり、もう一つは電子署名と関連した公認認証期間の責任を重くする電子署名法第２６条の規定［公認認証期間は認証業務遂行と関連して、加入者または公認認証書を信頼した利用者に損害を与えた場合は、その損害を賠償しなけ

ればならない。但し、その損害が?可抗力により発生した場合は、その賠償責任が軽減され､公認認証機関が過失の無いことを立証した場合には､その賠償責任は免除される。]である。

しかし、まだ本事案と類似した情報セキュリティに関連する問題に対して、民法第７５０条に対する特側によって不法行為に関する規定をおいてはいないので、結局この問題は、一般不法行為の原則により解決されることになる。

一般不法行為の成立要件は、１）故意又過失、２）違法性、３）責任能力、４）損害の発生など４つである。この中で主に問題になるのは１）と２）である。

その中でも故意または過失が特に重要な要件であり､故意というのは､「自己の行為により一定の結果が発生すろであろうとのを認識しながら、その結果の発生を容認して敢えてその行為をするという心理状態」を意味しており、過失とは､「ある行為により一定の結果が発生すると知りうるにも関わらず、それを知らないでやったという場合」に認定されるものである。過失では、その概念的前提として、注意義務があり、この注意義務違反が過失になる。

ところで、過失に関しては、その前提となる注意義務の種類によって、抽象的過失と具体的な過失の区別がある。抽象的過失とは、「善良な管理者の注意」が欠けた過失で、具体的な過失とは､「自己資産と同一の注意」が欠けた過失である。不法行為における過失とは、その中の「抽象的な過失」をいう。

それは一方では、通常人として行わなければならない注意をしていれば足りるし、その場合、もっと周到綿密な注意をしていれば損害の発生を防止できたとしても過失はない。しかし、それはもう一方では、注意力が足りない者であっても、通常人として行うべき注意を行わなかった場合には、過失があることになる。

しかし、抽象的な過失といっても、非常に抽象的、一般的に過失を考えることは適当ではない。例えば、自動車運転者については、運転者に通常必要となる注意義務が基準となることであり、それを離れて「通常人」を考えることは無意味である。

即ち、通常人というのは、その職業、地位における通常人を意味するのであり、過失の認定に関しては、その事件の性質や環境も当然。考慮することになる。一方、ある地位に対して、法により、ある作為義務または不作為義務を課する取り締まり規定を設けてあれば、それもその地位にいる人の注意義務を構成することになる。法に明示的な規定がなくとも、いわゆる社会常識または条理に照らして、特定の地位または立場にある人に、一定の注意義務があると認定する場合もある。ところで、このような部分は不法行為の成立要件中、違法性と連結され得るものである。

上記のような過失の概念を注意義務違反と見なす場合、その概念には事実上、違法性の概念も含めることになることが分かる。即ち、注意義務違反が認定されると過失と違法性が当時に認定され得るものであり、そのように取り扱って違法性を別途に検討しないで、注意義務違反の可否だけを検討するのが韓国の判例の立場である。これは日本の場合と違わない。

従って、実際の不法行為訴訟において１）注意義務が認定されること、２）その注意義務に違反したこと、３）損害が発生すること、４）損害発生と注意義務違反の間で相当の因果関係があること等の四つの要件を審査することになる。ここで基本的に重要なことは、注意義務の認定の可否である。本質問において問題になる事案を解決するにあ

たっても、その要諦は結局、注意義務が認定されるかどうかにある。
　これに関連して、各責任主体別にどのような基準で判断しなければならないかに対しては、後の該当する質問に回答しながら詳細に言及することとし、ここでは、上記の質問で提示されたいくつかの質問に対して回答することにする。

　まず、（a）ソフトウェアまたはハードウェアに欠陥があった製造者、開発者の責任に対する問題を検討する。この問題は後で言及する製造物責任法に基づく製造物責任と関連してよくみかける問題でもある。しかし、製造物責任は一定の要件のもとで、民法第７５０条の一般不法行為規定に対する特側を規定したものなので、その特側規定の要件を充足していない場合は、再び民法第７５０条の一般不法行為の要件に該当しているかを検討することとなる。ソフトウェアの場合、製造物責任法の適用対象物である「製造物」に該当するかに対する疑問はあるが、ソフトウェアの欠陥に対しても一般不法行為の成立は完全に排除するものではないと考えられる。問題は、ソフトウェア製造者が社会常識上、このような欠陥のあるソフトウェアを市場に出さない注意義務があるといえるかどうかにある。それは具体的な事案ごとに、異なる結論が出る可能性がある問題であり、一律に断定してはならない。例えば、会計プログラムを作って市場に出したのに、そのプログラムの重大な欠陥により会計が不正確になって、購入者が被害を受けたら、場合によっては不法行為責任が認定され得るであろう。
　不法行為責任と製造物責任のもっとも大きな違いは、加害者の故意過失を立証する必要があるか否かである。被害者が製造物の欠陥に対して不法行為責任を主張するのだとしたら、多くの場合、故意・過失の立証に苦労することになるであろう。それが製造物責任法の立法趣旨でもある。

　次に(b)下流責任の問題について検討することにする。韓国で下流責任に関して別途の法規定があるわけではない。この問題も上で明らかにした「注意義務違反」があるか否かの観点から原論的に解決するしか他にない。即ち、情報セキュリティに対する侵害攻撃を停止することに失敗した最初の被害者の責任の有無を検討するに当たって、その人が被害者であるというのは、絶対的な意味を持ち得るのではない。その人自身が被害を受けたこととは関係なく、他の被害者たちとの関係で、自分が情報セキュリティに対する攻撃を予防したりシャットアウトしたりする処置を行う注意義務があったにも関わらず、これを履行しなかったことにより、被害を発生させたり拡大したりした場合であれば、不法行為責任を負わなければならない。この場合に重要なのは、その一次的被害者の地位、技術的な対処可能性、その他いろいろな事情に照らして、法令または社会常識上、注意義務があるといえるかどうかである。これも同じく、具体的な事案別に個別的な判断を下すべきで、一律に断定することはできないが、そのような注意義務の存在とその違反に基づいた損害発生が認定されて、不法行為責任を負う場合もあり得ることを排除することはできないであろう。以上の観点は、韓国の法令、判例に照らして大きな疑問がものではないと考えられる。特に、公開されたパッチを設置することを怠った場合や、広く知られている脆弱性に対する適切な処置を行うことができるのに、そうしないことにより、多数人に被害を与える場合であれば、責任が認定できる可能性は多いと考えられる。

次に（C） システムにおける脆弱性を発見するため、効果的な監査を怠った場合の責任に対しては、上記の（b）において言及し、明らかにした内容が基本的に適用されることになり、おそらくは、政府の責任と関連した問題に繋がるようであるが、その部分は後述の責任主体別の論議において再び言及することとする。

（２）債務不履行（契約責任）

債務不履行責任と関連して、韓国の民法第３９０条は、「債務者が債務の内容に従い履行を行わない場合には損害賠償を請求することができる。但し、債務者の故意や過失なしに履行できなくなった際にはこの限りでない。」と規定している。但書規定により、故意、過失のない場合は債務不履行責任を負わなくなるが、それが但書規定にあるため、立証責任は、故意、過失がなかったことを主張する債務者にあるものと解釈される。それが不法行為責任と大きく異なる部分である。

そして、不法行為責任は加害者と被害者の間で契約関係があるかの有無には関係なく、上記で説明した要件だけが充足されると認定され得るのに反して、債務不履行責任は原則的に損害賠償請求者とその相手の間の契約関係を前提としているという点に重大な要件上の違いがある。

例えば、ISP と PC 喫茶店業者またはインターネットショッピングモール業者などの間で、インターネット専用線サービス契約などが締結されていて、その専用線サービスが一時的に麻痺してしまった場合、一旦、債務不履行責任が問題になり得る。

その際、ISP が責任を免れるために、「ISP の故意、過失などの責任ある事由がなかった。」という点を積極的に立証しなければならない。不可抗力によることだという主張は、帰責事由を否定する主張の一例であるため、その立証責任は ISP にある。

上記で関連質問として提示された事項に対して、ここでも少し言及しておく。

(a)ソフトウェアまたはハードウェアに欠陥があった製造者、開発者の責任は、その製造者また開発者と被害者（一次被害者を含む）などの間で契約関係が存在しない限り、契約責任としての債務不履行責任は問題にならない。直接供給者として供給契約を結んでいたとしたら、供給契約の相手との間で瑕疵担保責任が問題になり得る。例えば ISP へ供給したハードウェアまたソフトウェアに欠陥（瑕疵）があったとしたら、韓国民法第５８条、第５７５条に従い、購入者側から損害賠償請求をするか、それによって契約目的を達成することができない場合には、契約解除をし得る権利がある。しかし、このような権利は購入者に限られ、他の二次、三次の被害者とは無関係である。その場合、不法行為責任また製造物責任が問題になる余地があるだけである。

次に、(b)下流責任の問題について見るならば、契約責任においても、情報セキュリティ侵害攻撃を停止することに失敗した最初の被害者が、自己の顧客に対して負担するインターネットの正常な運営と提供に関する債務の不履行について、その者が最初の被害者であるということだけで免責を主張することはできない。自分が受けたその被害は自己が注意義務を履行したとしても免れることができない「不可抗力」の事件であったことを立証した場合に限り、責任を免れることができる。それは即ち、その者が自己に故意、過失がないことを立証しなければならないという原則に対して、例外にならないことを意味しているのである。

最後に、(c)システムにおいて脆弱性を発見する為、効果的な監査を怠った際の責任に対して見てみると、その監査義務を契約関係によって負担した場合であれば、契約責任（債務不履行責任）を負わなければならないし、そうではない場合は債務不履行責任の問題ではないといえるであろう。

（３）製造物責任

韓国では２０００年に製造物責任法を改訂したが、その立法的背景と重要な内容は次の A～H の通りである（法律全文は添付資料#4 を参照）。本質問と関連した事項は I において言及する。

A．立法的背景

製造物責任(Product Liability, PL)とは、欠陥がある製品によって、消費者また第三者の身体上、財産上に損害が発生した場合、製造者、販売者など、その製造物の製造、販売の一連の過程に関与した者が負担すべきの損害賠償責任をいう。

製造物責任法が立法化された背景を考察して見ると次の通りである。

１９７０年代以降、産業社会の急激な発展、現代科学技術の高度化などで製造物の欠陥による事故が頻繁に発生した。その後、１９７７年に、製造物責任に関する問題解決のため、韓国民事司法学会において製造物責任を論議して以来、多くの研究結果が発表され、裁判所では、製造物責任の問題を、過失責任主義に基礎をおいた現行法の不法行為責任の枠内で解決しようとする試みがあった。

しかし､学会においては､現行法の解釈を通して製造物被害者の救済は不十分であり、外国においても製造物責任法の立法化傾向が進んでいることを理由として、国内消費者の保護と企業競争力の強化という目標を達成するため、製造物責任法制定の立法の必要性を提議することになった。

そして、２０００年1月２１日に公布され、２００２年 7月 1日に施行された法律第６１０９号製造物責任法が誕生することになった。

立法化された製造物責任法のもっとも大きな意義は、被害者の被害証明負担が軽減したことで、それを始めとし、下記で、製造物責任法に特有の内容中、①製造物責任法の対象となる製品、②責任主体および、③製造物責任を問うことができる場合と、④損害賠償を受けうる被害の範囲、⑤製造者の免責自由ならびに責任期間の問題などを検証する。

B．製造物の概念

製造物責任法の対象になる製品は､「他の動産や不動産の一部を構成する場合を含んだ製造また加工された動産」である（製造物責任法第 2 条第 1 号)。従って、製造・加工ではなく、生産の対象と考えられる、一次農産物（林、蓄、水産物を含む）は本法の適用の対象にならない。また、機械・エアコン・ボイラーなど、それ自体の販売ではなく、器具の設置に瑕疵が有ったとしても、製造物責任法に基づいて責任を問うことはできない。

そして、「動産」の意味は、不動産を除外した全てのものをいい、一定の形態を持った個体・液体・気体のような有体物は勿論、形態がない電気とその他、管理し得る自然力も含まれている。但し、アパートやビルのような不動産それ自体は、本法の適用対象にならない。しかし、不動産の一部を構成しているとしても、照明施設、配管施設、空調施設など、個別的な動産は本法の適用対象に含まれる。

C．責任を問える場合

製品により事故が発生したとしても、無条件に製造業者の責任を認定するものではない。被害者は製品に欠陥があり、その欠陥により被害が発生した場合だけ製造業者に製造物責任を問うことができる。

製造物責任法上の「欠陥」とは、製造物の性質、使用方法などに対する説明、指示、警告その他の表示など、合理的に予想し得る当該製造物の使用形態、製造者などが当該製造物を流通させる時期など、あらゆる事情を考慮して、製造物に通常期待できる安全性が欠如することを意味する（製造物責任法第２条第２号）。

製造物責任において、欠陥はあくまでも製品の安全性に関する概念であるため、単純な製品の性能不足、品質不良のような、安全性に直接関わりがない、品質上や機能上の問題とは区分されている。

製造物責任を認定し得る製造物の欠陥は次のように分類できる。

①製造上の欠陥（製造物責任法第 2 条第 2 号ア目）

製造過程での不注意により、製品の設計仕様や製造方法に従わずに製品が製造されて安全性が欠如した場合をいい、このような欠陥は製品の製造、管理段階における人的、技術的不注意によるものである。例えば、品質管理の不良、安全装置故障、組み立て状態の検査不良、部品不良などが挙げられる。

②設計上の欠陥（製造物責任法第 2 条第 2 号イ目）

製造物の設計段階で安定性を十分に配慮しなかったため、製品の安全性が欠如した場合で、その設計により製造された製品は全て欠陥がある事と見なすことができる。例えば、安全設計不良、安全装置不備、重要原材料および部品の不適合などが挙げられる。

③表示上の欠陥（製造物責任法第 2 条第 2 号ウ目）

消費者の使用または取扱い上、一定の注意をしなかったり、もしくは不適当な使用をした場合などに発生し得る危険に備えて、適切な注意や警告を行わない場合をいうものであり、製造者はその製造物の使用から発生し得る危険に対して警告を行わなければならない。例えば、取扱説明書・警告事項の不備、表示不良（拡大・詐欺）、警告不適切などが挙げられる。

上記の三つの種類の欠陥を判断することに当たって、①危険の頻度および大きさと比較した当該製品の有用性、②損害発生の蓋然性および損害の深刻性、③製造業者また販売業者が当該製品を供給した時期、④合理的に予見し得る当該製品の用途および使用形態、⑤危険を防止するための設計・表示などの技術的・経済的実現可能性、⑥その他当該製品の安全と関連した事項などを総合的に顧慮しなければならず、必ずしも、製品の絶対的な安定性を要求するものではない。

D．責任主体

製造物責任法は、製造の欠陥による損害に対して賠償責任に問われる者を「製造業者」と規定している（製造物責任法第 2 条第 3 号)。「製造業者」としては、①製品を直接的に製造・加工した者と、②製品を直接的に輸入した者が中心となる。勿論、輸入品に対しては当然に直接、外国で製品を製造・加工した者に対しても損害賠償を請求することができる。

また、PB 商品や OEM 商品のように、直接製品を製造・加工しなくても、製品に商品名・商号・商標その他の表示をし、自己を製造業者・加工業者・輸入業者として表示し、もしくは誤解を招く表示をしている者も製造業者と見なされ、本法により責任を負わなければならないというのが一般的な解釈論である。

E. 損害賠償責任

製造物責任法において損害賠償とは、製造者が欠陥のある製造物により生命、身体また財産上の損害を受けた者に対して、その損害を賠償する責任を問うことをいう（製造物責任法第 3 条第 1 号)。製造業者は欠陥と相当因果関係がある全ての損害に対して賠償しなければならない。被害者は製品の欠陥で生命を失ったり、身体、健康を害した場合は勿論、財産の被害を受けた場合、損害額の多少を問わず、全ての損害に対して賠償を請求することができる。

製造物責任は現行民法第７５０条の不法行為責任の「故意また過失」の要件を「欠陥」で換えたものである。民法上の不法行為責任においては、被害者が損害賠償を請求しようとすれば、製造者の故意また過失を立証しなければならない。

しかし、製造物責任においては、無過失責任を採択した。その理由は、産業社会の急激な発展により、製品が高度化・専門化する反面、被害消費者は製造工程および使用方法などに関する情報が足りないため、損害賠償請求要件事実の立証が難しくなったからである。そのため、製造物の欠陥・損害、そして欠陥と損害との因果関係だけ立証するようにし、消費者の負担を軽減したのである。

最後に、本法による損害賠償責任を排除したり制限しようとして、製造業者および販売業者と消費者の間で締結した契約は無効である。これは、製造業者などがあらかじめ自己の責任を制限する特約を約定しても効力がないようにすることで、消費者を保護するためである。但し、被害者が事業者の場合、人間の生命、身体ではなく、営業用資産に対して発生した損害について、製造業者と被害者間で締結した免責特約の効力は、例外的に認められている（製造物責任法第 6 条)。

F. 連帯責任

同一の損害に対して賠償する責任がある者が２人以上の場合は、各自が連帯してその損害を賠償する責任がある（製造物責任法第５条)。即ち、部品の欠陥により損害が発生した場合、部品製造業者と完成品製造業者が連帯して責任を負うことになる。連帯責任において被害者が誰に損害賠償を請求するかは自由で、実際上は、最も財力がある者を

選択することになる。
　まず賠償をすることになった者は、他の連帯責任者に対して内部的な責任比率に基づき求償権を行使することができるが、他方に支給能力がなければ、まず賠償した者が負担を甘受しなければならない。

G. 製造者などの免責

　製造物責任は絶対責任では無いため、製造物に欠陥があった場合であっても、一定の理由に当該し、製造者がこれを立証した場合には、製造物責任に基づいた損害賠償責任責任を免れることができる（製造物責任法第 4 条)。但し、これは製造物責任法においての責任を免除するという意味であり、民法やその他法律による賠償責任まで免除するものではない。

　製造者の免責事由を見てみると次の通りである。
　①製造者が当該製品を供給していない事実が挙げられる（製造物責任法第 4 条第 1 項第 1 号)。盗難された製品のように、製造業者がその製品の供給に関与しない製品に対して被害が発生した場合がこれに当該する。
　②製造業者が当該製品を供給した時の科学・技術水準では、欠陥の存在を発見することができない事実である（製造物責任法第 4 条第 1 項第 2 号)。これはいわゆる、「開発危険の抗弁」を規定したもので、開発上の危険に対して損害賠償責任を認める場合、研究開発や技術開発が低迷し、究極的に消費者に損害を与えることになるのを顧慮したものである。製造業者がこの開発危険の抗弁を主張し、責任を免れるためには、当該製品の欠陥の有無の判断が必要となり、入手可能な最高水準の科学・技術の知識に照らして、欠陥であるということを認識できなかったことを証明することが必要である。
　③製造物の欠陥が、製造業者が当該製品を供給する当時の法令に定めてある基準を遵守しながらも発生した事実である（製造物責任法第 4 条第 1 項第 3 号)。しかし、「KS」マークや「品」、「検」字マークなど、安全関連マークを受けたとか、形式的承認などを受けた事実だけでは製造業者は責任を免除されることはできない。
　④原材料、部品の場合は、当該原材料や部品を使用した製品製造業者の設計または製作に関する指示により欠陥が発生した事実である（製造物責任法４条第 1 項第４号)。これは原材料、部品製造業者だけに適用される免責事由である。しかし、このような免責事由が認定されたとしても、製造業者が製品を供給した後に製品に欠陥が存在する事実を知ったか、もしくは知ることができたのにも関わらず、その欠陥による損害の発生を防止するための適切な処置をしなかったのであれば、本法による責任の免除を受けることはできない（製造物責任法第４条第２項)。

H. 製造業者の責任期間（消滅時効など）
　期間の経過により製品生産に関する各種記録や証拠が消滅すると、訴訟時に被告（製造者）の防御が困難になり、無限に暫定的な責任追及が続くことになるならば、製造者の合理的な製品開発計画や経営計画の樹立が難しくなる。従って、損害賠償責任が永遠に存続することを防止し、製造者の法的安定性を確保する見地から、一定の期間が経過

すると損害賠償請求の権利を否定する必要がある。現行民法上、不法行為責任においては、一定の期間が経過した際には損害賠償請求権を行使する事ができなくなるようになっており、製造物責任においても損害賠償請求件の消滅時効を認めている（製造物責任法第７条)。
?損害ならびに製造者などを知ってから３年（製造物責任法第７条第１項)
製造物責任の損害賠償は被害者またその法廷代理人が損害ならびに損害を発生させた製造者を知った時から３年以内に請求しなければならない。従って、３年が経過した場合、損害賠償請求権は時効で消滅となる。このように時効期間を設けたのは傷害または損害が発生して被害者側は製造者に対して損害賠償を請求できる権利があるのにも関わらず、その権利の上に眠ることと、製造者が無期限に損害賠償を請求されることを防止するためである。
②製造者などが製造物を供給した日から１０年（製造物責任法第７条第２項)
製造者が損害を発生させた製造物を供給した時から１０年が経過した際には損害賠償請求権が消滅になる。例外的に、この期間は身体へ蓄積された場合に人間の健康を害す物質による損害、または一定的の潜伏期間が経過した後で症状が現れる損害、例えば医薬品や化学製品のように、その服用また使用から被害発生まで、長期間の時間がかかる場合などに対しては、その損害が発生した時から起算することになる。製品が市場で使用されている限り、いつでも製造者は製造物責任を負担する危険を受けることになるので、このような製造者の不安定を解消するために、製品は製造また販売されてから一定期間が経過すると、それ以降には製造者や販売者を一切の賠償責任から解放する制度をおくこととなった。

Ｉ．本質問と関連事項

情報セキュリティと関連して、欠陥があるハードウェアまたはソフトウェアの製造者が、製造物責任法に基づいて製造物責任を問われるのか否かについて考察してみる。
まず、ソフトウェアの場合を見ると、ソフトウェアが製造物責任法上の製造物の概念に含まれているかについて、多くの論議がある。上記で明らかにしたように、製造物責任法の対象となる製品は､｢他の動産や不動産の一部を構成した場合を含んだ製造また加工された動産」と規定されているので、まず、動産に当該していなければならないことは明らかである。動産には有体物以外に、形態がない電気とその他管理できる自然力も含まれているが、例えばソフトウェアが有形的な媒体で固定された状態ではなく、オンラインを通して無形の情報だけで移転する場合には、このような無形的情報形態のソフトウェアを電気・その他管理できる自然力に当該すると見なすことができないので、製造物責任法の対象になり得ないことが比較的に明白だと判断される。しかし、ソフトウェアが CD-ROM パッケージ形態に固定された状態で販売された場合は見解が分かれる可能性がある。現在、韓国で訴訟が提起されている SQL-Slummer 事件の場合、原告代理人は、SQL　Server プログラムの製造者であるマイクロソフト社を共同被告として訴訟を提起しながら、それが CD－ROM形態で販売され、動産に当該するとの理由で、基本的に製造物責任を問い、補完的に不法行為責任を問うという方式で、請求原因を構成した（添付資料#9、#10、#11 参照)。

ハードウェアの場合は、動産に当該する事に疑問が無いため、製造物当該性を巡っての論難は起きないものと予想される。

製造物当該性に問題がない場合は、結局、その欠陥が製造物責任法でいう欠陥に当該し、被害者らが受けた財産上の損害が、その欠陥と相当因果関係にあるか否かが重要なイシューとして取り扱われることとなろう。

２．刑事責任など

（1）情報通信基盤保護法の規定

情報通信基盤保護法では、重要通信基盤施設に対する電子的侵害行為と関連して、次のような刑事処罰規定と過料規定を設けてある（条文内引用条文などは添付資料#1参照)。

①重要情報通信基盤施設撹乱などの行為に対する処罰（法、第２８条）

次の行為を行い、重要情報通信基盤施設を撹乱、麻痺また破壊した者は１０年以下の懲役また1億ウォン以下の罰金に処する。

１．アクセス権限を持たない者が、重要情報通信基盤施設へアクセスしたり、アクセス権限を持った者が、その権限を越えて保存されたデータを操作・破壊・隠匿また流出する行為

２．重要情報通信基盤施設に対してデータを破壊したり、重要情報通信基盤施設の運営を妨害する目的でコンピュータウィルス・論理爆弾などのプログラムを投入する行為

３．重要情報通信基盤施設の運営を妨害する目的で、同時に大量の信号を送ったり、不正な命令を処理するようにするなどの方法で、情報処理に間違いを発生させる行為

上記の規定において情報通信基盤施設とは、国家安全保障・行政・国防・治安・金融・通信・運送・エネルギーなどの業務と関連する電子的な制御・管理システムおよび「情報通信網利用促進ならびに情報保護などに関する法律」第２条第１項第１号の規定による情報通信網をいう（上記、法、第２条第１号参照；

一方､｢情報通信網利用促進及び情報保護に関する法律｣第２条第１項第１号には､｢『情報通信網』とは、電気通信基本法第２条第２号の規定により、電気通信設備を利用したり、電気通信設備とコンピュータおよびコンピュータの利用技術を活用して、情報を収集・加工・保存・検索・送信また受信する情報通信体制をいう。」と定義している)。

結局、インターネットなど、情報通信網自体が情報通信基盤施設に含まれるということが分かるが、上記の処罰規定はその中でも「重要」情報通信基盤施設（重要情報通信基盤施設の指定と関連しては同法第８条参照）を撹乱、麻痺、破壊した場合を適用対象とし（結果的加重犯）、続いて２号、３号の場合の重要通信基盤施設の運営を妨害する目的を要件とすることで(目的犯)、以下から分かるように、一般的なコンピュータウィルス流布などの行為に比べて、かなり加重された処罰を科している。

②秘密漏洩に対する処罰（法、第２９条）

第２７条の規定を違反して秘密を漏洩した者は５年以下の懲役、１０年以下の資格停止また５千万ウォン以下の罰金に処する。

③過料（法、第３０条第１項）

次の各号の何れかに当該する者は１千万ウォン以下の過料に処する。

１．第１１条第１項の規定による保護処置命令を違反した者
２．第１６条第２号の規定による通知をしていない者
３．第２０条の規定による申告をしていない者
４．第２２条第２項の規定を違反して関連書類また資料を提出していない若しくは虚偽に提出した者
５．第２３条第２項の規定を違反して記録及び資料を返還するかもしくは廃棄していない者

（２）情報通信網利用促進ならびに情報保護に関する法律の規定

情報通信網利用促進ならびに情報保護に関する法律では、一般的な情報通信網侵害行為などに対して次のような処罰規定を設けている（法律全文は添付資料#５参照）。

①情報通信網の侵害行為など

正当なアクセス権限なしに、あるいは許容されたアクセス権限を越えて情報通信網に進入した者は３年以下の懲役または３千万ウォン以下の罰金に処する（情報通信網利用促進ならびに情報保護に関する法律、第６３条第１号、第４８条第１項）。

正当な事由なしに情報通信システム、データまたプログラムなどを毀損、滅失、変更、偽造し、または、その運用を妨害できるプログラム（悪性プルグラム）を伝達または流布した者、情報通信網の安定的な運営を妨害する目的で大量の信号またデータを送り、もしくは不正な命令を処理するようにするなどの方法で情報通信網に障害を発生させた者は、５年以下の懲役また５千万ウォン以下の罰金に処する（上記、法、第６２条第４号、第４８条第２項、第６２条第５号、第４８条第３項）。

②情報毀損、秘密侵害

情報通信網によって処理、保管また転送される他人の情報を毀損したり、他人の秘密を侵害、盗用また漏洩した者は５年以下の懲役また５千万ウォン以下の罰金に処する（情報通信網利用促進ならびに情報保護に関する法律、第６２条第６号第４９条）。

（３）刑法規定

①コンピュータ関連業務妨害

コンピュータなど情報処理装置また電子記録など特殊媒体記録を損壊し、もしくは情報処理装置に虚偽の情報または不正な命令を入力したり、その他の方法で情報処理に障害を発生させ、その業務を妨害した者は５年以下の懲役、または１千５百万ウォン以下の罰金に処する（刑法、第３１４条第２項）。

ウィルスを侵入させる行為、メール爆弾またスパムメールなどでシステムに過負荷を招来する行為、正常な命令語を使用してサービスを過度に要請するサービス拒否攻撃行為（Denial of Service　Attack, DOS Attack）、インターネットを転々としてシステムの性能を低下させるインターネットワームを流布させる行為、一定の条件が充足されると

システムを破壊する論理爆弾を使用する行為などと共に、電話交換機システムを撹乱させるフォンプレーキング(Phonephreaking)も本罪に当該する事例とされている。

②秘密侵害
封緘、その他の秘密の処理をした人の手紙、文書、図面または電子記録など特殊媒体記録を、技術的手段を利用して、その内容を調べ出した者は、３年以下の懲役また５百万ウォン以下の罰金に処する（刑法、第３１６条第２項）。

3.2.2：法的責任の要素(Elements of security legal liability)
情報セキュリティ、機密性、正確性、可用性と法的責任には、どのような関係がありますか[IT5]。

【回答】質問の趣旨を正確に理解することが困難であるが、結局、過失の可否を検証するときに、どのような注意義務があったかということが重要な判断要素になることが上記で明らかになったのであって、その注意義務と関連して情報セキュリティの機密性などいろいろな状況が具体的、個別的に考慮されると考えられる。

3.2.3: 主体的側面(Subjective aspect)
情報セキュリティに対する侵害があった場合に、被害者から責任を追求され得る当事者についてあげて下さい。
具体的に[IT6]以下の例について記述して下さい。

【回答】
・ハッカー(脆弱性に対して攻撃するソフトウェアを開発し、意識的に配布するもの)：
民事的には故意の不法行為をしたものと評価され、被害者などがそれに基づいて被ることになるあらゆる損害を賠償しなければならない。刑事的には状況により上でみたところに同じく、刑法上のコンピュータ関連業務妨害罪、電子通信網利用促進ならびに情報保護に関する法律上の情報通信網侵害行為などに該当し、それに従って処罰され、されにそれが重要情報通信基盤施設を撹乱、麻痺または破壊する結果をもたらす場合には情報通信基盤保護法上の処罰規定に抵触し､それに従った重い処罰を受けることになる。

・ 脆弱性の存在するハードウエアまたはソフトウエアの製造業者または開発者
特別な場合を除いては､刑事責任は問題にならず､民事責任の有無のみ問題となろう。上で見たところと同じく、ハードウェアの場合は製造物責任法上の「製造物」に該当することに疑問がなく、そのハードウェアの欠陥によって受けた被害者は製造物責任法に基づく損害賠償請求ができることになろう。ソフトウェアの場合には、無形的な情報自体だけでは、製造物ということはできず、製造物責任法の適用対象ではなく、それをパッケージして CD－Rom など有形的媒体に保存し、流通させた場合にも、故意または過失で欠陥（脆弱性）があるソフトウェアなどを製造、販売して他人が被害を受けたと認定されれば､民法上の不法行為責任を負う場合がありうる。また、製造者から商品を直接、購入した購入者との関係では、欠陥のある製品の引渡しが不完全履行であるという理由

で、債務不履行責任を負わなければならない場合がある。さらにそのソフトウェアなどに瑕疵があり、その瑕疵の存在事実を購入者が知らず、知らないことに過失がなかった場合には、民法上の瑕疵担保責任を問える場合もあり得よう。但し、一般的な債務不履行責任であれ、瑕疵担保責任を問いうることは、直接的な契約当事に限られ、他の第三の被害者はこうした主張をすることはできない。

・ コンサルタント、システムインテグレーター、配布者、販売業者、その他脆弱性有る技術を推奨したベンダー

脆弱性のある技術を推薦したコンサルタントなどがその技術を導入した側との間で、一定の対価のもとにコンサルティング業務を適正に遂行する契約を締結しているのに、こうした契約上の義務を負担していて、その義務を適正に履行していないものと認定され、契約の相手方がそれに基づき損害を被った場合であれば、その相手方に対して、債務不履行責任を負わなければならない。他の第三者である被害者に対しては彼らに対する一般的な注意義務を欠く故意、過失が認定される場合に限り、民事責任が問題となりうる。

・ セキュリティの評価やセキュリティ脆弱性の回避を委任されたコンサルタント

この場合、コンサルタントがセキュリティの評価を誤り、セキュリティの脆弱性を回避する義務を十分に履行しなかったか、履行しなかったことにより、委任者側が損害を受けた場合には、債務不履行責任を負わなければならない。場合によっては、一般的な故意、過失が認定される場合には、第三の被害者たちに対しても、不法行為責任を負わなければならない場合があり得る。

韓国では、スラマーに関連して提起された訴訟では、大韓民国（情報通信部）が共同被告のひとりになっているが、これは、重要情報基盤施設を管理する機関の長（この事件では情報通信部長官）が、この基盤施設の脆弱性を分析し、回避するための措置をとる法令上の包括的義務を負担しているという点を前提としたものである。もちろん、この事件では、原告が勝訴するためには、情報通信部が実際の法令上の注意義務に違反していたということと、それが被害者たちの損害との間に相当因果関係があるということを主張、立証しなければならない。事件はまだ、準備手続きの段階である。

・ 脆弱性を発見する監査人

この監査人は、脆弱性を発見すれば、即座にこれを回避するための措置をとらなければならない契約上の義務を持っているが、これを履行しなかったことにより被害を惹起した場合であれば、契約上の債務不履行責任を負わなければならず、こうした義務を法令または社会常識（条理）によって負担している場合では、不法行為責任を負う場合があり得る。

・ 攻撃を抑止するように依頼していたセキュリティ・プロバイダー

契約によって依頼をうけたセキュリティ・ロバイダーが、契約上の義務を十分に履行しなかった場合には、契約上の債務不履行責任を負うことになり、彼らが対外的な面でも故意、過失があることを認定された場合には、第三の被害者たちに対する関係でも、

不法行為責任を負うことになる場合があり得る。

・ アプリケーションを最新に、パッチを宛ててもらうことにしているアプリケーション・サービスプロバイダー

ASP サービス提供会社が、ソフトウェアの脆弱点を保管するパッチファイルをあてずに、ハッキングなどの攻撃を受けた場合には、原則的にそのサービス利用者に対する関係で債務不履行責任を負わなければならない可能性が高く、過失に基づく不法行為責任も免れるのは難しい場合が多い。

・ システムをアウトソースしている場合のホスティング会社

システムをアウトソーシングしている場合であっても、ホスティングサービスの顧客に対する関係では、アウトソーシングしているという理由だけで債務不履行責任を免れることはできない。不法行為責任の有無を判断するにあたっては、前述した一般的な原則の他に、使用者責任の有無に対する法的判断が必要になる。これに対する韓国の法制度は日本の場合とほぼ一致する。

・ 攻撃を許容し、または、停止し得なかったISP

上記で、「下流責任」と関連して説明した部分が、この部分に対する回答に代えることができよう。

具体的な状況に従い、個別的に注意義務違反の有無を判断しなければならず、後で説明する、「情報通信サービス情報保護の指針」が注意義務の有無を判断するにあたって、重要な参考になる法規上の基準であるということができる。この指針はによると、その注意義務は侵害事故の予防に関する注意義務を、侵害事故発生時の迅速で適切な対処に関する注意義務に分けられる。

・ （追加）IDCセンター

韓国の「情報通信網利用促進ならびに情報保護に関する法律」第４６条によれば、「①他人に情報通信サービスを提供するために集積された情報通信施設を運営、管理する事業者は、情報通信施設の安全な運営のために、情報通信部令が定めるところにより、保護措置をとらなければならない。

②第１項の規定による事業者は、集積された情報通信施設の滅失、毀損、その他運営の傷害によって発生した被害を補償するために、情報通信部令が定めたところに従い、保険に加入しなければならない。

③情報通信部長官は、第１項の規定による保護措置をとらない事業者に対し、相当な期間を定め、是正措置を命ずることができる。」と、規定している。いわゆる、サーバの賃貸を業としている、IDC センターの場合、上記のような保護措置をなおざりにして事故が発生した場合には、それに従って、債務不履行ならびに不法行為責任をおわなければならない。

・ 脆弱性を発見していながら、それを被害者、ベンダーまたは公に報告しなかった者

報告しなかったすべての人が法的責任を負うのではない。契約上、明示的にあるいは

黙示的に、報告義務を負っている場合には、契約上の債務不履行責任を、法令または条理上の報告義務が認定される場合には債務不履行責任を負うことになる場合がある。

韓国の情報通信基盤保護法では、情報保護コンサルティング専門企業に対して、一定の保護義務ならびに記録保存などの義務を賦課している（同法、第２２条、第２３条など参照）。情報保護コンサルティング専門企業がこうした法令上の義務に違反したことが侵害事故の原因である場合には、不法行為などの責任を負う場合があり得る。

3.2.4. 脆弱性の場所

以下のような脆弱性の発生個所によって、責任を問われる人が異なりますか？
- クライアント側
- サーバ側
- ネットワーク機器部分
- など

【回答】これに関する特別な規定があるわけではないが、民法などの一般原理を適用して責任主体による責任の有無、特に注意義務違反の有無を検討するに当たって、上記のような脆弱性発生位置の問題は、かなり重要な要素となるであろう。クライアント PC において脆弱性が発生したら、サービス提供者側に責任を問うことは難しい場合が多いであろう。サーバ側に脆弱性があるのなら、これを利用し、顧客にサービスを提供する会社ならびに関連ハードウェアの製造者などの責任が問題になるし、ネットワーク機器部分に脆弱性があれば、機器製造者や納品業者側の責任が問題となる外に、その機器を利用してインターネット接続サービスなどを提供している会社側に責任がある可能性が多いであろう。

以下のようなソフトウェアの提供形態によって、責任の違いを区別しているかを解説してください。
- パッケージ品ソフトウェア（市販品）
- 個別開発品ソフトウェア
  - 外注（成果物検収 Deliverable）
  - 委託（工数検収 Labor hour）
- サービス提供に利用しているソフトウェア
- など

【回答】やはりこれに対する特別な規定は別にあるわけではなく、民法などの一般原理に基づいて判断しなければならない。上記で明らかにしたように、パッケージ商品中に、有形的な媒体（動産）に固定された形態で提供された場合には、製造責任法の適用対象になり得るという主張があるが、これに対して、まだ判例が出たことはない。もし、これが判例によって承認されたら、製造物責任法の適用の可否と関連して、CD などの有形的な媒体に固定されたパッケージ形態の販売と、そうではない場合とは、かなりの違いをでることになるであろう。

3.2.5　注意義務－標準(Duty of care-standard)

3.2.5.1 一般(general)

法によって情報セキュリティの基準が定義されていますか。
脆弱性の改善義務についての基準を法令等で設けているか？
法令等以外の情報も知っていれば教えてください。

【回答】情報通信網利用促進ならびに情報保護に関する法律（及び同法施行令、施行規則）において、情報通信網における情報保護に関する一般的な規定をおいている（上記、法律および施行令、施行規則全文は添付資料＃5、＃6、＃7参照）。

上記、情報通信網利用促進ならびに情報保護に関する法律第５２条第１項は、「政府は情報の安全な流通のため、情報保護に必要な施策を効率的に推進するために、韓国情報保護振興院（KISA）を設立する。」と規定し、同条第３項において、KISA の業務を規定し、その中の一つに、＜情報保護システムの性能と信頼度に関する基準制定ならびに標準化支援＞を揚げている（同項第５号）。

また、上記、法第４７条第１項は、「情報通信サービス提供者および情報通信サービスを提供するために物理的施設を提供する者は、情報通信網の安定性および情報の信頼性を確保するために樹立運営している技術的・物理的保護処置を含む総合的管理体系（以下、「情報保護管理体系」と呼ぶ）が、当該サービスに適合するか否かに関して、第５２条の規定による韓国情報保護振興院から認証を受けることができる。」と規定し、情報保護管理体系認証制度を設けている（２００１．７．１．施行）。

上記規定によって韓国では、KISA の主導で情報保護に関する標準の制定ならびに認証業務を遂行している。

特に情報保護管理標準（TTAS.IS-17799）は、「情報保護管理体系認証制度」の基礎となるもので、国際標準 ISO/IEC 17799 を応用して、韓国情報保護振興院（KISA）が国内実情に合うように開発したものであり、それまで適切な保安管理指針書がために業務遂行に難しさを感じてきた保安管理者は勿論、認証審査機関の業務遂行について指針書の役割を果たすことを期待されている。

3.2.5.2. 管理者の義務[IT7] (Duties of administrators)

システム管理者が、不具合を修正するためになすパッチやソフトウェアを使用することを怠った場合、責任があるか。
システム管理者がセキュリティ情報を収集するのを怠ったとき、責任があるか。

【回答】「情報通信網利用促進ならびに情報保護に関する法律」第４５条第１項は、「情報通信サービス提供者は、情報通信サービスの提供に使用される情報通信網の安定性および情報の信頼性を確保するため保護処置を準備しなければならない。」と規定し、同条第２項は、「情報通信部長官は、第１項の規定による保護処置の具体的な内容を定めた情報通信サービスの情報保護に関する指針を定め、公示して、情報通信サービス提供者にその遵守を勧告することができる。」と規定していて、この規定による情報通信サービスの情報保護指針が情報通信部により公示されている（添付資料＃8参照）。

このような規定により、全ての情報通信サービス提供者は、情報通信網の安定性および情報の信頼性を確保するため、保護処置を準備する法的義務があり、その具体的な保護処置については、上記指針に規定された内容が一つの基準として適用されるであろう。少なくとも注意義務の有無を判断するにあたって、上記の指針は重要な基準として働くものであろう。ところで、上記指針によると、情報通信サービス会社は、システム管理者と情報保護責任者を指定しなければならないし、情報保護責任者は脆弱性に対して周期的な点検、分析および報告義務を負っている。このような義務の内容には、保安脆弱性に対するパッチプログラムが出たという情報を適時に入手して、これを活用するべき義務も含まれているものと解釈されるので、これを怠った場合には、注意義務に違反したことになり、相手によって、不法行為または債務不履行責任を問われる可能性が高いであろう。

3.2.5.3 インシデントにおけるシステム管理者の義務（Duties of system administrators in case of incidents）

インシデントに対応する際、システム管理者は、不十分な対応しかできなかった場合、または、対応がおくれた場合、責任を負うか。

損害を回避する責任を負う当事者が他にいますか。

【回答】これは情報セキュリティに対する侵害事故を予防するための注意義務ではなく、侵害事故発生時の適切な処置に関する注意義務と関連するものである。情報通信サービス情報保護指針第８条第５項によると、サービス提供会社により指定された情報保護責任者は、周期的にアクセス記録を分析して侵害事故を予防し、侵害事故を発見した場合には直ちに必要な処置を取らなければならないと規定されている。この中で、後半部分がこれに当該する。情報保護責任者が直ちに必要な処置を取らなければならないという注意義務を怠ったことにより、顧客などに被害が発生し、または拡大した場合には、情報通信サービス会社としては、債務不履行責任と共に、不法行為に対する使用者責任に基づいて損害賠償義務を問われる場合が多いであろう。侵害事故時の対応が一見不十分に見えても、現在の技術水準としては、それ以上の対処が不可能な場合であれば、注意義務が認定される範囲を超える場合として、責任を免れることになるであろう。

情報保護責任者が被用者の場合には、契約責任は会社自体が負担し、不法行為責任は会社と担当責任者が不真性連帯責任を負うことになろう。

この他に、情報保護業務を第三者に依頼した場合にも、契約責任は依頼した会社にあり、不法行為責任は依頼を受けた会社が問われる場合が多いであろう。

3.2.5.4. セキュリティ・ポリシー(Security policies[2])

1　注意義務の標準として、セキュリティポリシーを必要としていますか。

[2] In this context,” security policies” have broad meaning and include “Implementations, Planning and Audit”cycle.

【回答】注意義務の基準となる情報保護基準は必要なものと認識されており、上述のように、「情報通信サービス情報保護指針」が制定されている。

２　保険会社や産業界の事業者協会で、ガイドラインを標準としていることはないですか。

【回答】政府および傘下機関の法規、指針以外に産業会のガイドラインは発見なかった。

３　セキュリティポリシーの実際の運用が責任に対する抗弁になりますか。

セキュリティポリシーの実際の運用が連邦ガイドラインのようにコンプライアンスの観点から考えられていますか。

【回答】情報保護業務の法規の基準を遵守したのであれば、債務不履行責任に関連して帰責事由がないと抗弁をするの大変助かることになり、不法行為に関連しても法規上の注意義務は遵守したものと認定される可能性が高いと思われる。事業者が自主的に作ったセキュリティポリシーがある場合、これは法規上の基準に照らして正当性が認定される場合に限ってこのような効力があると思われる。

４　セキュリティ上の脆弱性が、セキュリティの監査および評価をしていながら、それを探知できなかった場合、その監査および評価をしていた事実は、抗弁となりえますか。

【回答】「情報通信サービス情報保護指針」第８条第４項においては、「情報保護責任者は、周期的に情報システムの保安脆弱点を点検、分析して、その結果を情報通信サービス提供者に報告しなければならない。」と規定されているので、情報保護責任者が情報システムの保安脆弱点を周期的に点検、分析しているのであれば、これ自体が上記指針上の（注意）義務を遵守している部分であり、損害賠償請求訴訟において有力な抗弁事由の一つとなり得る。しかし、通常の情報保護責任者であれば十分にその脆弱点を探知することができたのにも関わらず、これを行っていない場合には、過失が認定され、債務不履行または不法行為責任を免れ得ない可能性が高い。

3.2.6 その他(Miscellaneous)

１　セキュリティ・インシデントの実体を明らかにするのに有効だと考えられる法的システムはありますか。

【回答】公共機関が持っている情報に対しては、公共機関の情報公開に関する法律において、一般国民に「情報公開請求権」を認める規定が設けられている。この法律に対して市民団体などでは、まだ情報公開の範囲などが微弱であるとして、全面的な改正を主張されている。その他 ISP、重要ソフトウェア製造者などに対しては、情報公開請求制度が認められておらず、ただ民法訴訟が提起される場合に「文書提出命令」の申請など

により、一定の情報の提出を強制し得る方法があるにすぎない。
逆に、情報通信部など政府機関の立場からは、事故の実態を素早く把握するため、ISPが持っているログ資料などの提出を要求する権利を持ちたがっている。韓国におけるSQL-Slummer事件が発生した後、情報通信部では、このような方向の立法を推進すると話しがもちあがり、これに対してプライバシー侵害を警戒する市民団体の強い反対意見が提起された事がある。

２　「内部告発者保護」や「司法取引」の法制度を有していますか。

【回答】最近、韓国の政府（財政経済部）は、会計情報に対する企業の責任強化法案として、公示書類虚偽記載を指示した場合に関連した内部告発者保護規定を導入するという方針を明らかにしている。尚、法務部は、権力型非理（不祥事）剔抉（暴き出すこと）のための腐敗監視システムの一環として、内部告発者の身分保障、申告者の免責などを制度化するという方針を明らかにしている。しかし、また推進段階であり、具体的な立法成果が表われているわけではない。上記のような会社支配構造および、権力型不祥事に関連した問題の他に、一般的な内部告発者保護制度の必要性は、市民団体を中心として提起されているが、いまだに確かな結論を出してはいない。情報保護に関連した内部告発者保護制度については、いまだに韓国では大きく論議されてはいないものと思われる。
アメリカの法廷映画でよく見られる「司法取引」は、韓国国民の情緒には、合っていないと考えられるし、これに対しては導入論議が全く見られない。

３　「内部告発者保護」や「司法取引」の法制度が、セキュリティ・インシデントの実体を明らかにするのに有効と考えられるのではないかという議論はありませんか。

【回答】韓国で上記の二つのイッシュは、上記で述べたように情報保護問題に関連しては、特別な論議の焦点にはならなかった。

3.3 責任有る開示の問題(Responsible disclosure issue)

１　脆弱性に気がついたとき、気がついた人間は、会社や公的機関に報告すべき義務がありますか

【回答】「情報通信サービス情報保護指針」第８条第４項は、「情報保護責任者は、周期的に情報システムの保安脆弱点を点検、分析して、その結果を情報通信サービス提供者に報告しなければならない。」と規定している。
その他に公的機関に報告する義務を規定している法規はいまだにない。後で詳しく紹介する情報通信網利用促進ならびに情報保護に関する法律改正案には、上記のような報告義務を拡大する規定が含まれている。

２　報告された会社などは、これに対して対応すべき義務はありますか。また、対応をなしうる体制をとっておく義務があると解されていますか。

【回答】「情報通信網利用促進ならびに情報保護に関する法律」および、それに基づく、「情報通信サービス情報保護指針」によると、このような対応義務および管理体制構築義務があると解釈される。

　このような部分も、後で紹介する情報通信網利用促進ならびに情報保護に関する法律改正案において、より強化された形の義務規定に変っている。

３　産業界や政府の機関が、脆弱性がわかった際に、それに対して責任有る開示となるようなガイドラインを準備していますか。もし、準備している際は、その内容をお教えください。

【回答】責任ある公開に関連した論議は、韓国であまり見られないようである。但し、情報通信基盤保護法においては、中央行政機関の長と、長から委任を受けた管理機関の長が、重要情報通信基盤施設の脆弱点の分析、評価、対処などに関連して、組織的、行政的支援のいろいろな処置および方案を講ずることができるよう、根拠規定を設けている（添付資料参照）。

４　脆弱性の報告について、その内容を分析する専門的な委員などの制度が提案されていませんか。もし、議論されているのであれば、その内容をお教えください。

【回答】情報通信基盤保護法第９条においては、重要情報通信基盤施設に対する脆弱点の分析、評価に関連して、「専門チーム」を設ける根拠規定を準備している。その他には、別の論議についてはわからない。

3.4 SQL Slummer の事件をきっかけに何か動きなどがありましたか？

【回答】

[? ?] ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? '? ? ? ? ? '(SQL-Slummer ? ?)? . ? ? ? ? ? ? ? ? ? ? . (? ? ? ? ? '? ? ? ? ? ? ? ? ? .hwp' ? ?)

［回答］韓国情報通信部においては、最近、いわゆる「インターネット大乱」（SQL-Slummer 事件）を契機に情報保護関連規定を大幅に強化することを重要内容として含んだ、情報通信網利用促進および情報保護に関する法律改正案を出し、公聴会などを通して世論を収斂している。その内容は次の通りである（添付資料中の「網法改正関連資料.hwp」参照）

A．改正の背景

o　情報化の進展により、各社会部門がネットワークで相互連結され、政府、企業、その他団体および個人の活動は、情報システムとネットワークに絶対的に依存している。

- しかし、情報システムとネットワークにより保存、伝達される情報は、非認可アクセスによる使用、誤用、変造、悪性コード転送、サービス拒否またはシステム破壊のような多様な危険にさらされている。

o 特に、去る１月２５日のインターネット侵害事故は、従前のサイバー攻撃と異なり、ネットワーク自体を攻撃し、急速にインターネット網全体に障害を発生させる新たな形態に変化した。

- いまや情報保護は特定な部門の問題ではなく、情報システムとネットワークを利用する政府、企業、利用者全体の問題に拡大し、皆が総体的に協調してこそ、効果的な対応が可能である。

o また、最近、個人情報管理が杜撰なために流出する事例が発生するなど、個人情報保護に対する不安感が大きくなり、個人情報保護に対する管理的処置の強化が必要となった。

o したがって、インターネットの公共性を勘案し、インターネットの安全性、信頼性を確保して、インターネットを利用する各利用者の責任と役割を提高する（高める）ため、関連法律の改正を推進する。

B. 経過および重要内容

1）推進経過

o 2003.3.13 ：情報通信網保護対策政策討論会開催
- 重要政策法案発表、および関係専門家などからの意見収斂

o 2003.3.28 ：大統領年頭業務報告
- インターネット侵害事故対応支援センター設置、情報保護事前評価制導入などを報告

o 2003. 4 ：情報通信網保護対策新部計画樹立

o 2003. 5 ：法律改正　専門作業チームの構成、および改正案初案の準備

- 2003.5.27　重要内容を情報通信基盤保護実務委員会に報告

2）重要な改正の内容

□　侵害事故関連重要改正内容

o インターネット侵害事故発生時における迅速な対応と原因分析

- インターネット侵害事故対応支援センターの設置とその役割

- ISP、IDC、アンチウィルス業者などに対して、侵害事故を迅速に報告するようにし、侵害事故原因分析などのために、ログ記録保存命令制、現場調査権、資料提出要求権などを規定した（これに対しては上述の通り、市民団体－一緒に動く市民行動－などからプライバシー保護の側面での強い批判に直面している）。

o 個人、企業、政府など各部門別に情報保護を強化する。

- 現在、IDC だけに保護処置を義務化しているが、ISP、IDC、大衆利用施設などに対して細分して、情報保護安全基準を賦課し、これを遵守するように義務化を規定した。
※情報保護コンサルティング専門業者などを通して周期的な安全診断を実施し、KISA の安全診断基準および技術開発、遠隔診断サービス提供などの業務を規定した。

- 情報通信施設が集中している IDC の場合、重大な侵害事故の発生時に、IDC が、入居している業者のサーバに対し、異常トラフィックの遮断などの緊急処置を行う権限などを付与した。

- ISP を通じた利用者情報保護処置の強化

- S/W 業者には、保安パッチ情報を購買者に２回以上告知させることとした。

o 情報保護投資拡大の推進

- 政府、地方自治団体などが一定規模以上の情報化事業を推進するとき、企画段階から情報保護要素を反映できるよう、「情報保護事前評価制」を導入した。

o ハッキング、ウィルス流布など、サイバー犯罪の処罰を強化した。

o その他情報保護産業、情報保護産業協会の根拠規定の準備など

（個人情報保護に関する改正規定についての紹介部分は省略する）

3.5 「ソフトウェアの脆弱性に対応するガイドライン」の観点でご意見があれば教えてください。

特別な意見はなし。

以上

第2　その他の資料
1　ソフトウェアの脆弱性をめぐる法律問題

ソフトウェアの脆弱性をめぐる法律問題

弁護士　高橋郁夫

1.　議論の契機

従来のソフトウェアの脆弱性の問題については、議論はあったものの、これは、万人に公開されるべきであるとするいわゆる完全開示原則とでもいうべきものが適用されていた。しかし、これが今現在、正面から議論されるべき問題として認識されている。

この議論が正面から、議論されるようになったのは、おそらく２０００年７月２６日のラスベガスにおける“Black hat Security Conference”における Marcus Ranum 氏の”Script Kiddies Suck“ [3]という講演からだと思われる。Ranum 氏は、その講演の中で①セキュリティに対する認識を変更すべきこと②問題を開示する方法を変更すべきこと③アカウンタビリティーを変更すべきことを説いている。

①セキュリティに対する認識を変更すべきことというのは、「スクリプトキディ」が多数おり、一般大衆は、彼らにうんざりしていること、そして、彼らの数を減らさなくてはならない、そのようにセキュリティの考え方を変更しなければならないということを説いている。そして、ハッキングは、アマチュア・テロリズムだといい、容赦なく対応しなければならないとしている。そして現在は、ホワイトハットとブラックハットとの間にを非常に大きなグレーのエリアがありこのグレーのエリアを減らさなくてはならない、元ハッカーをセキュリティーコンサルタントとして雇うのを止めなければならないといっている。

②完全開示の変更について、彼は、完全開示の方法は、スクリプトキディの大軍を作り、ソフトウェアの品質に何らのポジティブな影響を与えず、バグを訂正するためのポジティブなインパクトを与えるものではないという点で自己欺瞞だったという。脆弱性の情報の進化の過程は、別紙のとおりであるが、欠点（情報以前のもの）があり、脆弱性があり、それが現実化し、公開されず、ツールが生まれ、スクリプトキディがこれを利用する。その一方で脆弱性の公開により発見・評価の論理がなされ、パッチが作られ、ユーザがこのパッチをインストールするという過程を経る。そして、彼は、スクリプトキディは必要悪でありうるかという疑問を呈し、ソフトウェアには自動アップデートのシステムを設定しうるし、公表するにはよりよい方法があるので、スクリプトキディがユーザにアップデートをなすよう強制しているとかベンダーがミスを隠すのを不可能にしているということは言えないとしているのである。そして、完全開示の神話として４つのことがあるという。（１）ハッカーはこれらの記述をすでに知っており、彼らがなしうるテクニックをすべての人が知りうるのがベストである。（２）ベンダーは、ひとたび公開されれば彼らのバグを隠すことはできない。（３）情報は将来におけるよりよいシステムをつくるために公開することが必要である。（４）そしてそれは自分自身の財産である。これらの神話に対して彼は、（１）確かにハッカーはそうであるがスクリプトキディはそうではない。脆弱性の大多数は、公開されるために調査され、公開されるので

[3] http://www.blackhat.com/presentations/bh-usa-00/MJR/MJR-blackhat-2000-keynote.ppt

ある。（2）欠点を公開する効果的な他の方法がある（3）詳細を教えたりテストしたりする必要はない。（4）自分の財産だといっても、を自分の宣伝、財産的利益、エゴのメッセージなどである。

③セキュリティに関連する問題のアカウンタビリティーのレベルを増加すべきであるという主張もなされた。ツールなどをリリースする人間は、彼らの行動の結果に対して責任を取るべきであり、また、セキュリティのバグを持った製品を生産するベンダーは、修正を提供する標準を守らなければならない。

これらの考察をもとに、彼は、自分が正しいかどうかは明らかではないとしながら、以下のような点などを予言として指摘するのである。（1）グッドガイは、敵に対して戦闘なすであろう。（2）攻撃ツールの作者と頒布者は、民事損害賠償訴訟において高い判決額を受けるであろう（3）従来の法執行機関のよりハッキングに対応する試みは、民事裁判のおかげで放棄されるであろう。

そして、結論として、私たちは、インターネットセキュリティ時代の始まりの終わりにいると思うとしている。フン族は、ローマのなし方をしらずに、その吸いつくし方を知っていたにすぎないということを覚えておくべきであるとしている。

２．　議論に対するリアクション

この議論は、大きな反響を巻き起こしたようである。Weld Pond, ZDNet/USA の記事[4]によれば、「Ranum氏は，聴衆の神経を逆なでしたに違いない。あらゆる人が，カンファレンスの基調を定めるものとして同氏のスピーチを話題にしていたが，私が話をした一部の人たちが示した「基調」は，ある種の怒りだったからだ。」とされているのである。彼は、この問題提起に一定の理解をしめしつつも、「情報公開を排除すれば，問題はさらに悪化するだけだ。」として、「セキュリティ研究情報の自由な交換を抑えつけようとするのではなく，ベンダーにモチベーションを与え，より安全な製品が開発されるよう協力して取り組む必要がある。出荷される製品に，過去の問題が潜在的な脆弱性として再び含まれることがないようにする必要がある。ユーザがセキュリティホールをすばやく簡単に修復できるようにするという課題にも，協力して取り組む必要がある。攻撃者がセキュリティ問題を発見してそれを悪用できるのなら，善良な人々の側が，先に問題を見つけて修復できるような，より良い方法がきっとあるはずだ。」としている。

3.脆弱性の論点をめぐる提案

その後、このソフトウェア脆弱性の問題は、その後、セキュリティコミュニティや各ベンダーにおいて、積極的に、重要な問題として認識されるようになっていった。２００１年８月には、Russ　Cooper氏は、完全開示原則が、悪意有るコードの拡散をたすけたのではないかという問題提起をなしており、１１月には、NT BugTrack 上で責任ある開示フォーラムを作るという提案[5]をなしている。

また、Microsoftのセキュリティ対策センターの Scott Culpは、その２００１年 10月に発表した「It’s time to end　Information　Anarchy」[6]という論文において、「セ

[4] 「セキュリティ情報の公開は是か非か」（http://www.zdnet.co.jp/news/0008/22/pond.html）
[5] http://www.ntbugtraq.com/default.asp?sid=1&pid=47&aid=66
[6]

キュリティコミュニティは、これらの兵器を構築する青写真を提供するのをやめる時期に来た。コンピューターユーザーは、セキュリティコミュニティに対してユーザを保護すべき義務があると主張すべき時期に来ている。私たちは、セキュリティ脆弱性を議論することができ、そして、すべきであるが、私たちは、賢明で、スマートで、責任ある方法でなすべきである。」といっているのである。彼は、まず、すべてのセキュリティの脆弱性を排除できないのであれば、脆弱性情報を慎重にかつ責任をもって取り扱うことが重要になるという。ところが実際にセキュリティコミュニティが、取り扱っているやり方は、良くいって情報アナーキー等いうべき方法である。そしてこの点の実務とワームの近ごろの動きは関係しており、脆弱性情報の詳細の公表は、兵器として利用することに貢献しているのである。

情報アナーキーは、近ごろにおけるベンダーがセキュリティ脆弱性を公に明らかにする点についての進歩のほとんどをやり直す脅威を有しているのである。もし、脆弱性を公に明らかにすることが不可避的に脆弱性が利用されることにつながるであれば、ベンダーは、彼の顧客を守るために他の方法を探すしかなくなるのである。これは、脆弱性を議論することを止めることを求めているではなく、他の人人々をリスクにさらすことを超えるものは何かという線引きをしようとしているのである。表現の自由をあきらめるをという行っているのではなく、混雑した映画館で火事だと叫ぶのをやめさせようとしているだけなのである。この問題は、セキュリティコミュニティ自体よりも問題が大きく、すべてのコンピューターユーザーは、利害関係を有しているのであり、私たちは、みんな、脆弱性情報が、適切に取り扱われることを確かにするのを助けることができるのである」といっているのである。

このような論考の立場と呼応するかのように Microsoftは、カリフォルニア州マウンテンビューにセキュリティの専門家やプライバシー擁護派，政治家などを集め，「Trusted Computing Conference」と銘打ったカンファレンスを開き（２００１年１１月６日から８日まで)、そこで、「システムの脆弱性の情報開示」という基本原則を改めようとする動き[7]をさらに強化するように考え[8]、さらに、そのメンバーと団体を設立する動きを見せた。

4.議論の発展と混迷

具体的な脆弱性の報告のプラクティスをめぐっては、上記の議論をめぐっていろいろな提案がなされている。なお、この点については、この議論が一般化する前から、CERT/CCにおいて、「脆弱性公開ポリシー」として明らかにされていた[9]。

これらの 議論のうちもっとも注目すべきものは、IETF における「バグ報告ガイドライン」であろう。このガイドラインの内容は、IETF の HPからは、既に削除されていて[10]、詳細は、不明である。なお、報道記事などを前提にすると、責任ある開示プロセスのた

---

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/noarch.asp

7 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/standard.asp

8 http://www.zdnet.co.jp/news/0111/07/e_relief.html

9 http://www.kb.cert.org/vuls/html/disclosure

10 http://www.ietf.org/internet-drafts/draft-christey-wysopal-vuln-disclosure-01.txt

めの最善の手法を提示することを目的とするものである。そのプロセスは、具体的には、以下のようになる。セキュリティ研究者は，ソフトの脆弱性を発見したら，それを開発元に報告するか，開発元と連絡が取れない場合は， CERT/CCなど，信頼できる第三者セキュリティ機関に報告する。開発元は報告を受けたら，7日以内に回答する。あるいは，報告に対する返信を自動化している場合は，より具体的な回答をいつ返せるかを明記する必要がある。またこの場合，具体的な回答は10日以内に行うこと。ソフトメーカーは7日ごとに，研究者に対して当該問題に関する最新情報を提供し，報告から30日以内に問題を解決できるよう努めなければならない。また、すべてのソフトメーカーに対して，「secalert@companyname.com」のように、セキュリティ専門家からソフトの脆弱性に関する警告／通知を受け付けるためのメールアドレスを別途用意することを提案している。

そして、この特徴は、報告者に対しても一定の責任を要請するものとしての傾向が堅調なところにある。具体的には、「ベンダーが30日以内に脆弱性を解決するのが困難な場合もある」という点をバグ報告者が理解すべきだと指摘し、具体的には、次の3つのケースが挙げられるという。1つは，バグがセキュアではない設計に起因するものの場合。2つめは，バグが影響するハードウェアやOS，サポートすべき製品のバージョンが多数に及ぶ場合。3つめは，ベンダーがセキュリティ技術に熟達していない場合である。これらの場合には、「上記のケースに当てはまる場合には，ベンダーが誠意を持って脆弱性の解決に当たっている限り，報告者はベンダーに時間的猶予を与えるべきだ」とこの草案には記されている。

もっともこの提案に対しては、批判も強い。「こうした方針を採用すれば，ベンダーがこの草案の条件を盾に，自社のバグウェアを棚に上げて報告者に『無責任』のレッテルを貼ることになりかねないという。」のである。

そして、このガイドラインは、3月18日に、IETFの管轄外として取り下げられた。

その後も、この点をめぐる議論は続き、2002年10月には、前述のMicrosoftが設立の動きを見せていた団体であるOrganization for Internet Safety」という団体が設立された[11]。しかしながら、具体的な活動については、そのHPなどを見る限り、未知数である。

現時点におけるこの論点の議論は、いまだ混迷を続けていると評価することができそうである。ここで、一つの事件を紹介することができる[12]。この事件は、ソフトウェアの著作権と第三者のセキュリティホールの公開についての法的問題という形式をとったものである。AutoProf.Com社は、ScriptLogic社のツール（Windowsのクライアントを中央から環境構築する）に無権限で管理者アクセスを可能にする脆弱性があることをホワイトペーパーで明らかにした。 ScriptLogic社は、2002年８月に、AutoProf社を、リバースエンジニアリングおよび、悪意有る宣伝を企てることにより、著作権法およびライセンス契約違反で訴訟を提起した。この訴訟については、原告と被告が、競争相手ということもあり、開示の適切性を直接に争点とするものではないが、しかし、開示のルール自体の必要性を強調するものだという評価があり、そのような指摘は、的外れとはいえないであろう。

---

11 http://www.oisafety.org/

12 http://www.gcn.com/21_34/security/20634-1.html

6.最後に

再度、Marcus Ranum 氏の問題提起に移ることとする。そこでは、刑事的手法による規制よりも民事的な判決例の積み重ねによる脆弱性をめぐる利害関係の調整が期待されているように思われる。そして、特に脆弱性の侵害に対して、高額の損害賠償による一定の判断が、提唱されていた。

しかしながら、このような問題提起について見れば、現時点では、あまりあたっているとはいえないようである。セキュリティをめぐる然るべき技術的措置を取るべき法的義務という観念は、いまだ、一般化していないようにも思え、また、米国においても、なかなかそのような義務が問題になった法的事案の報告を見かけないのである。

Ranum 氏の民事的な判決例の積み重ねによる脆弱性をめぐる利害関係の調整という問題意識が、はたして、現実化してくるのか、成り行きが注目されるものと言うことができるであろう。

『セキュリティホールに関する法律の諸外国調査』報告書

付録　Ｂ－５

ドイツ　報告書日本語訳

（余白）

情報セキュリティにおける責任に関する質問書への回答

Universität Münster
Prof. Dr. Thomas Hoeren

I. 課題の説明

この調査の目的は、日本の経済産業省に、情報セキュリティの侵害にかかるドイツにおける現行法規、判例ならびに指針について情報を提供することである。本報告書は、インターネットの分野に関してなされ、民事法上、刑事法上および行政法上の局面を考慮するものとなっている。

以下の想定される事例が調査の基礎となっている。
ある会社が別のある会社に対し訴えを提起したと仮定する。原告は、その情報システムがインターネットを経由して「Slammer」というウイルスにより損害を受け、被告のシステムがこの攻撃の原因となっていたということを主張する。しかしながら、原告は、被告のシステム自体が攻撃の被害者であったことは認めている。
被告が、このウイルスの拡散および被告のシステムの感染が生じないようにするための事前の措置を講じることを怠ったと、原告は主張している。
さらに、原告は、このウイルスの原因を創り出した者に対して、たとえばウイルスの拡散に寄与したすべての関与者に対しても、ソフトウエアの供給者に対しても、措置をとるつもりである。
みずからが場合によって原告に対して支払わなければならない損害賠償の求償をうるために、被告は、ウイルスの作成者とその供給者に対しても、アプリケーションの提供者に対しても、さらに追求する。
質問事項の課題設定は、ウイルスに関するドイツ法による様々な責任の可能性を以上の事例の想定を基礎として説明することである。

II. 質問の回答

3.1 定義
3.1.1 脆弱性(Schwachstellen)を議論する際に「ソフトウエア」という概念の定義が存在するか。
「ソフトウエア」の法律上の定義はドイツ法には存在しない。もちろん著作権法 69 条 a に「コンピュータプログラム」の概念に関する定義は存在している。

著作権法 69 条 a 保護の対象
(1) この法律の意味におけるコンピュータプログラムは、設計資料を含め、あらゆる形態におけるプログラムである。

これとは別に、ソフトウエア概念についての DIN の一覧表が存在する。DIN とはドイツ工業規格であり、ドイツ規格協会（登録協会・ベルリン）によって作成される。ドイツ規格協会は、「ドイツ工業規格委員会(DNA)」の事業団体であり、製品の計測、重量、素材、影響を及ぼす要因、色調ならびに質をいわゆる(DIN)規格表に統一的に確定することに関して権限を有している。
DIN-ISO は、その場合、ISO 規格（国際標準化機構）をドイツ語に翻訳したものであり、場合よっては従来の DIN 規格を逸脱することを指示している。

DIN/ISO 規格 9000、第 3 部の定義（ソフトウエアの開発、提供および保守に対する ISO9001 の適用のための便覧（1992 年））は次のように述べている。
「ソフトウエア：情報処理プログラムによる作業に属する、プログラム、プロセスならびにそれに属するすべての仕様書から構成される精神的製品（No. 3.109）

ソフトウエア製品：ユーザに提供するよう決められているコンピュータプログラム、プロセスならびにこれに属する仕様書およびデーター式全て」

したがって、ソフトウエアはコンピュータプログラムより広い概念であり、文書作成によって補完されたコンピュータプログラムを含んでいる。

3.1.2 「セキュリティホール」、脆弱性(Schadenspotential/ Schwachstelle)」および「不具合」を定義している法令等は存在しているか。

「セキュリティホール」および「脆弱性」については、ドイツの法令等で定義は存在しない。

「不具合(Fehler)」の概念について：

保証との関連において、ドイツ法では、「瑕疵(Mangel)」という表現が選択されている。

瑕疵概念は、売買、賃貸借および請負契約という三つのもっとも重要な契約類型において、比較的統一性があるが、法律効果の点だけは異なっている。

物に瑕疵があるかどうかを判断するにあたっては、当事者がなにを合意していたか、もしくは、その物が契約上前提とされる使用あるいは通常の使用に適しているかが、原則として重要となる。

ディスクまたはソフトウエアがウイルスに感染して引き渡された場合、ドイツ連邦共和国のラント裁判所のいろいろな判例によると、これは瑕疵を意味することになる。引渡しの時点でハードディスクがウイルスに感染している場合も、同様である。

欠陥(Fehler)の別の概念は製造物責任法3条1項、2項に存在する。

製造物責任法3条 欠陥(Fehler)

(1) すべての事情、特に

a) その提供、
b) 当然考えられうる使用、
c) 取引された時点

を考慮して、正当に期待することができる安全性を提供しない場合、製造物は欠陥を有している。

(2) 後に改善された製品が取引されたという理由だけでは、製造物は欠陥を有していることにはならない。

たしかにこの引用した規定には衡量すべきメルクマールが提示されてはいるが、しかしながら、この欠陥の定義はひじょうに抽象的に述べられている。ドイツ連邦議会の法務委員会は、しかし、この規定の不明確性を是認しただけでなく、実務で生じている製造物の欠陥の多様性が詳細な定義を許容せず、他方で、それぞれの個々の事案で裁判所に解釈をゆだねることができるという理由で、必要なものと考えていた。

裁判所は、過去に、犯罪としての製造物責任でまったく法律上の規定がなくとも機能的な欠陥概念を構成していた。

最後に、DIN6627 がソフトウエアの欠陥と供給者と顧客によるその判断を取り扱い、欠陥と瑕疵を評価する手続を提供しているということがさらに注目されるべきである。この手続は、当事者によって、契約の構成部分にすることが可能である。しかも、裁判における鑑定によって利用される。

3.1.3 「セキュリティホール」の概念が法令等で使用されていないか。

ドイツには、情報セキュリティにおける一般的な基準についての規定は存在しない。したがって、「セキュリティホール」の概念は関係法令等で使用されていない。

3.2 責任

3.2.1 一般的なフレーム

最初に、情報セキュリティにおける脆弱性ないしは瑕疵に関する責任についてのドイツ法の諸規定を概観することとする。

情報セキュリティにおける責任に関するドイツ法の諸規定の概要

以下の基本的な責任に関する規定は、ウイルスに関する責任に関係する民事法上の諸規定ならびに刑法上の諸規定に分かれる。それに続いて、さらに短く、行政の法律上の責任の可能性について説明をおこなう。

1. 契約法

ソフトウエアにウイルスが発生することによって、まず、契約違反が存在しうる。債務関係の内部で義務が有責に侵害されている場合、損害賠償請求権が生じる。この場合、そのような請求のための基本的な規定は民法 280 条 1 項である。別の条件（給付またはさらなる履行の期限の設定）のもとでは、債権者は給付にかえて損害賠償をも要求することができる。この場合、債務者は、それまでに給付したものの返還請求をする権限をもち、当然、債権者は、反対に、損害賠償の範囲内で逸失利益をも要求することができる。

債務者は、民法 276 条 1 項により、故意と過失を弁護しなければならない。その場合、故意とは違法な結果の認識と意欲である。取引上必要とされる注意を怠った者は過失で行為している（民法 276 条 2 項）。

しかしながら、民法 280 条による損害賠償請求の領域では、有責性のメルクマールに関して、挙証責任の転換が存在している。義務違反に関する債務者の有責性は、最初、推定されているが、しかし、義務違反を弁護する必要がないという証拠を提出することができる場合、債務者は免責される。

民法 280 条 1 項は、給付に関係する者が義務ではなく、民法 241 条 2 項による付随義務を侵害するかぎりにおいて、関係する。

付随義務は、なかでも、他方当事者の権利、法益ならびに利益を考慮すべきであるという両当事者の義務のことである。

このことから、当事者の助言および説明の義務が帰結されることがありうる。

民法 280 条の基本規定に対して、民法の特別の規定が参照されている。どの特別の規定が該当するのかということは、どの契約類型を当事者が選択したのかということに依拠している。

しかしながら、損害賠償請求については、上述のように、つねに義務違反を要件として必要としている。これを認めることができるのは、瑕疵が存在する場合である。瑕疵の概念は、たしかにそれぞれの契約の種類について詳細な点で異なってはいるが、しかし、基本的には物が危険の移転場合に約定された特性を有していないかぎり、瑕疵は存在する。特性が具体的に約定されていない場合、契約により前提とされている使用もしくは通常の使用が重要となる。

この場合、ウイルスの発生したソフトウエアは、原則として、瑕疵があるものと位置づけられるべきである。このことは、持続的な損害を惹起するウイルスだけでなく、モニタの信号あるいはスピーカへの出力によってソフトウエアの通常の利用だけを阻害し、あるいは、計算時間だけを要求するウイルスについても妥当する。つねに給付にかえての損害賠償の阻却にいたる些細な義務違反は、この場合、問題とされない。すくなくとも計算時間と記憶場所は要求されているからである。

ソフトウエアのウイルス発生に関係する債務者の有責性にとって、債務者の側で適切な費用と周知の方法をとったならば探知することができるようなウイルスと、新規性のゆえにこのことが場合により妥当しないウイルスとが区別されなければならない。

被害者に共同の責任が帰属されるということもありえる。被害者が損害を共同して惹起し、あるいは共同して責任があるという事情は、損害賠償請求を阻却するものではないが、しかし、その額を減少させることにな

る。その場合、賠償請求の義務は、その額により、損害がどの程度とくどちらの側によって惹起されたのかということに依拠する。

ウイルス感染の場合も、被害者自身が十分なウイルスプログラムによって備えなかったということがおそらく留保される。

2. 不法行為・製造者責任(Produzenthaftung)

損害賠償は不法行為の規定によっても考慮される。民法823条1項によると、故意または過失により他人の生命、身体、健康、自由もしくはその他の権利を不法に侵害した者は、それによって生じた損害を賠償する義務がある。ウイルスの攻撃の場合、その他の権利としての財産をたいてい侵害している。

この場合、不作為に関する責任が考慮されるのは、作為の義務が認められる場合である。このことは、とりわけ社会生活上の安全義務が存在する場合に該当する。

この社会生活上の安全義務違反を理由とする責任が特に問題となる場合は、製造者責任である。製造元業者は、ある者がその製品の利用によってこうむった損害について責任を持たなければならない。この場合、判例によって製造者の以下の義務が構成されている。

- ・設計上の義務。たとえば、システムが十分に安全ではない場合または安全性を調整する部分が通常のユーザ（特別の電子情報処理の知識のない者）にとって遮断される場合。
- ・製品監視義務。すなわち、個々の不具合をもって製造された商品の排除である。このことは、たとえば、ドイツでソフトウエアを国の特殊性に適合させることについて妥当する。
- ・インストラクション義務。たとえば、ユーザにセキュリティのリスクに注意を向けさせない場合に存在する。この義務は、製品を検査し（それゆえ、輸入者や販売業者も含む）、その際にこの検査義務を高度に認められるべき者だけが、製造者の製品を不具合がないと考えた場合にかぎり、果たすことができる。
- ・製品観察義務。これから帰結されるのは、周知のセキュリティ上の欠陥を回避し除去する義務である。

被害者は、この場合、挙証責任の転換に基づいて、損害が用法にしたがった使用において発生し、製品の欠陥に基づいていることだけを立証すればたりる。その場合、製造元業者の有責性は推定される。

しかしながら、製造元業者は、その製品の欠陥があらゆる期待可能な事前の予防措置をおこなったにもかかわらず回避不可能であったということを立証することができる場合、免責されうる。

以上のこととは別に、以下で述べる刑罰法規あるいはその他の保護規定との関連で、823 条 2 項による損害賠償請求が生じる。

3. 製造物責任

不法行為に基づく製造者責任とならんで、製造物責任法による請求権も発生することがある。この法律は製造物の損害に関する製造者の有責性に依拠しない責任を規定している。この法律による賠償義務は合意によって排除できないものであり、あらかじめ排除することも制限することも許されない。

製造物責任法による製造者として規定されるのは、実際の製造者、輸入業者または提供者である。製造物は、それが他の可動物または不可動物の一部を形成する場合でも、すべての可動物である。

上記の 3.1.2 で説明したように、製造物に欠陥があるのは、あらゆる事情を考慮した上で正当に期待することができる安全性を提供しない場合である。

製造物の欠陥によって、人が死亡し、身体または健康が侵害され、あるいは、物が損害を受けることが必要である。製造元業者の有責性はこの点に関して必要ではない。

しかし、欠陥のある製造物とは別の物に損害が生じないなければならない。それゆえ、製造物責任法による賠償義務は、製造物それ自体に生じた損害については適用されない。

その物は日常的に私的な使用または消費のためのもと決められており、被害者によってもっぱら使用されるものでなければならない。業務上の利用のために使用され、または、業務上投入される物は保護されない。そのかぎりで、製造物責任法による責任は私的なコンピュータ利用における損害に限定される。

物的損害の場合、被害者は、500 ユーロを限度に損害を負担しなければならない。500 ユーロまでの損害の場合は、被害者には製造物責任法による請求権がまったくない。

様々な責任阻却事由 製造物責任法 1 条 2 項）のなかで、ウイルスの感染の場合には、とくに製造物責任法 1 条 2 項 5 号が重要である。これによると、製造者の賠償義務は、製造者が当該製造物を流通においた当時の技術の水準によると、当該欠陥を認識することができなかった場合には、阻却される。完全に新種の、すなわちまだ解析されておらず、専門誌においてまだ述べられておらず、かつあらゆる最新のウイルス保護プログラムによってまだ検知されえないコンピュータウイルスの場合、この規定にしたがって、責任阻却が認められる。

4. 妨害排除および差止請求
ウイルスが発症する場合、ソフトウエアについて財産権の侵害も存在し、そのため、関係者に民法1004 条 1 項による妨害排除請求および差止請求の権利が帰属する。

民法 1004 条 妨害排除および差止請求権
(1) 占有の剥奪または不法な占有によるのとは異なった方法によって財産権を侵害した場合、所有権者は、妨害者について、侵害の排除を要求することができる。さらなる侵害のおそれがある場合、所有権者はその差止を請求することができる。
(2) 所有権者が受任する義務がある場合、請求権は排除される。

5. 著作権法
著作権法は、著作権として保護される成果物の侵害を防ぐ規定を含んでいる。しかしながら、そのためには、著作権として保護される成果物の侵害が存在することが前提となる。
コンピュータプログラムは、著作権法 69 条 a の法律上の定義により、あらゆる形態において保護される。著作権法 69 条 a 3項は、コンピュータプログラムの保護の可能性に関して、「独自の精神的創作」という意味での個性だけを要求している。これによれば、創作や構成の特別の高度さが要求されるわけではない。単純なプログラムであっても、まったく些細なものでないかぎり、著作権法上の保護を受けることになる。
以上のことを、1993 年 7 月 14 日の連邦通常裁判所は確認している(BGHZ 123, 208. 簿記プログラムに関して)。

著作権法 69 条 c 2号によると、著作権者には、コンピュータプログラムに対する翻案（改訂）をおこなう排他的な権利が認められている。
この権利は、現存のコンピュータプログラムへウイルスを移植されることによって、侵害される。

著作権法 97条 1項は、コンピュータプログラムに対して適切に適用されるべきである。これによると、著作権法により保護された諸権利の侵害がある場合（ウイルスの場合は著作権法 69 条 c 2号）、侵害者に故意または過失が負わされるかぎり、私法上の損害賠償請求権が著作権者に認められることになる。

6. 刑法上の規定および秩序違反
刑法上の責任に関しては、原則として、すべての構成要件要素に関する故意が必要となる。故意が存在するのは、すべての構成要件の実現の認識と意思が存在する場合である。
過失行為が処罰されるのは、法律がこれを明文で処罰してる場合にかぎられる。しかしながら、この点は、個々で説明する犯罪構成要件については問題にならない。

ここで述べる犯罪構成要件においては、法律が明文で指示している場合にのみ未遂も可罰的となる（刑法202 条 a の未遂はしたがって不可罰である）。

5.1 刑法典の諸規定
202 条 a データへのアクセス
(1) 自己のために用いることを決められておらず無権限のアクセスに対してとくに保護されているデータを権限なく入手しまたは他人に入手させた者は、3 年以下の自由刑または罰金刑に処する。
(2) 1 項の意味におけるデータは、電子的、磁気的またはその他の直接知覚しえない態様で蔵置されあるいは伝送されるものだけをいう。

保護されている法益は、情報に対する支配関係である。データは、その者のために用いることが規定されていない者の手にあるべきではない。刑法 202 条 a のデータの概念のもとでは、狭義のデータだけではなく、プログラムおよびその他の電子的に蔵置される情報も該当する。これらのデータは、無権限のアクセスを阻止するという目的を有する特別のコピーの保護をもたせなければならない。

303 条 a データの改変
(1) 違法にデータ（202 条 a）を消去し、隠匿し、使用不可能にしまたは変更した者は、2 年以下の自由刑または罰金刑に処する。
(2) 未遂は可罰的である。

この規定は、データの改変のない使用という利益を保護している。
刑法 303 条 a によると、権限なくデータを消去し、隠匿し、使用できなくしまたは変更した者が可罰的であることになる。コンピュータウイルスは、そのホストプログラムの呼び出しに際して、別のまだ感染していないプログラムへ繁殖する。このようにして、ウイルスは、このプログラムのデータを改変している。このことが権限ある者の同意あるいはその他の方法で正当化されないかぎり、刑法 303 条 a によるデータの改変の不法構成要件を充足する。
ウイルスが他のシステムに投入され、そのためそこでプログラムに巣くっている場合はすでに、刑法 303 条 a による既遂が存在する。というのは、そのことによってプログラムファイルに置かれたデータが変更されているからである。そのかぎりで、損害は重要ではない。
未遂も 2 項において処罰される。これがとくに考えられるのは、データの改変がまだ生じてはいないが、すでに十分既遂に近接している場合である。それゆえ、たとえば、ウイルスが他人のコンピュータの記憶媒体にもたらせているが、しかしまだプログラムに感染していない場合がこれにあたる。

303 条 b コンピュータ・サボタージュ
(1) 他人の設備、他人の業務または官庁にとって本質的に重要であるデータ処理を、
1. 303 条 a 1項による行為を遂行すること、または
2. データ処理装置もしくはデータ媒体を損壊し、破壊し、使用不可能にし、隠匿しあるいは改変する
ことによって、妨害した者は、5年以下の自由刑または罰金に処する。
(2) 未遂は可罰的である。

303 条 b 1項 1号の前提条件は、データ処理が本質的に重要である他人の業務、企業または官庁のデータ処理装置に関係しなければならないことである。このことは、簿記およびその他の業務上の運営を電子的なデータ処理に切り替えている企業および官庁の場合には、確実にほとんどつねに該当するであろう。したがって、ウイルスを企業または官庁のデータ処理装置にポーティングする場合、つねに5年以下の自由刑という厳しい刑罰を考えなければならない。

刑法 303 条 b 1項 2号にある他方の行為態様の場合、データ処理装置またはデータ媒体が実質的に侵害されなければならない。コンピュータウイルスを投入する場合、本号の方法は例外的な場合だけ考慮されることになる。おそらく、データが消去されただけではなく、ハードウエアに対する損害、たとえばハードディスク・クラッシュが惹起されるということが これにあたる。

そのほかにも、一定の場合には以下の条項により責任を考えることになる。

303 条 器物損壊 :ハードウエアの損害が意図されて生じた場合
223 条 傷害 :人的な損害が意図されて生じた場合
226 条 背任 :財産上の管理義務が存在することが前提となる
263 条 a コンピュータ詐欺 :財産上の利益が意図されている場合

5.2 その他の法律の規定

刑法典のほかにも、刑法上の規定が存在する。

5.2.1 競争法

不正競争防止法は競争保護法であり、ウイルス攻撃の特別な事案で構成要件として考慮されることになる。不正競争防止法 17 条は、企業の営業上または業務上の秘密を不誠実な侵害に対して保護するものとなっている。これには、電子情報処理(EDV)をもちいて管理されているデータも含まれる。この規定の射程範囲は、一定の人的範囲に、すなわち企業のオーナーに雇われているかあるいは不誠実な方法で秘密として保持されるべき事実を獲得した従業員にのみ向けられていることによって限定されている。

さらに、競争目的で、自己の利益から、第三者の利益のためにまたは損害を意図して所為がおこなわれなければならない。

不正競争防止法 17 条

(1) 従業員、雇用者または営利企業の見習いとして、雇用関係のゆえに自らに委託されまたはアクセス可能となっている営業上または業務上の秘密を、雇用関係が有効に継続している期間において権限なく競争目的で、自己の利益から、第三者の利益のためにあるいは当該営利企業の所有者に損害を加える意図をもってある者に知らせた者は、3 年以下の自由刑または罰金に処する。

(2) 競争目的で、自己の利益から、第三者の利益のためにあるいは当該営利企業の所有者に損害を加える意図をもって、

1. 営業上または業務上の秘密を
   a) 技術上の手段を使用すること
   b) 秘密を有体化される描写をこうせいすること
   c) 秘密を有体化した物を領得すること

によって、権限なく創出しまたは確保し、あるいは、

2. 1 項に列挙された手段または 1 号による自己または他人の行為によって営業上または業務上の秘密を入手しあるいはその他権限なく創出し、確保し、権限なく使用しまたは他人に知らせた者は、同様に処罰する。

(3) 未遂は可罰的である。

(4) とくに重大な事案において、刑罰は 5 年以下の自由刑または罰金となる。原則として、行為者が漏らす際に、秘密が外国で使用されることを知っている場合、または、自らが外国で使用する場合であるときは、とくに重大な事案が存在する。

ソフトウエアのウイルスの大多数の事案では、不正競争防止法 17 条の前提条件が充足されていない。しかしながら、企業に対して従業員によりウイルスの投入が意図されている事案については、この規定を考慮すべきものということができる。

5.2.2 データ保護

連邦データ保護法の保護の対象は、個人を、個人に関係するデータを扱うことによってその人格権が侵害されることから保護することである。人格権は、基本法1条1項と関連して2条1項に定められており、そのため、もっとも高度の保護利益のひとつである。これには、情報自己決定権も属する。個人は、自己に関係するデータに関する主であるべきであり、基本的にそのデータの使用について決定すべきである。

連邦データ保護法は、データの許されない使用に関連して、以下の責任規定を含んでいる。

連邦データ保護法 43 条 過料規定

(1) 故意または過失により

……

4. 28 条 5 項 2 号に反して、個人に関するデータを伝送しまたは利用した者（著者注：連邦データ保護法 28 条 5 項 2 号によると、その充足のためにデータが伝送されるものとは異なった者に対して処理あるいは利用することを許容していない。）

……

8. 33 条 1 項に反して、関係者に報告せず、ただし報告せずまたは完全には報告しなかった者（著者注：連邦データ保護法 33 条 1 項によると、関係者にそのデータの保存に際して報告しなければならない。）

……

は、秩序違反で行為するものである。

(2) 故意または過失により、

1. 権限なく一般的にアクセスすることができない個人に関係するデータを収集しあるいは処理した者、
2. 権限なく一般的にアクセスすることができない個人に関係するデータを自動化された手続によって引き出す準備をした者、
3. 権限なく一般的にアクセスすることができない個人に関係するデータを引き出し、あるいは、自動化された処理によりもしくは自動化されていないファイルから入手しまたは他人に入手させた者、

……

は、秩序違反により行為したものである。

(3) 秩序違反は、1 項の場合、25,000 ユーロ以下の過料を、2 項の場合 250,000 ユーロ以下の過料を科すことができる。

個人に関係するデータは、連邦データ保護法の法律上の規定によると、特定されたまたは特定可能な自然人（当事者）の人的または物的な関係についての詳細な記述をいう。たとえば、氏名、住所、家庭状況、職業、身分証明書番号、電話番号がそうである。

連邦データ保護法 44 条 刑罰法規

(1) 43 条 2 項に列挙された故意の行為を代価をえて、あるいは、自己もしくは他人の利益を図りまたは他人に損害を加える目的で遂行した者は、2 年以下の自由刑または罰金に処する。

(2) 所為は告訴により訴追を受け、当事者、責任のある部署、データ保護に関する連邦代理人および監督官庁が告訴の権限をもつ。

5.2.3 著作権

著作権法からは以下の刑罰の規定が考慮される。

著作権法 106 条 著作権により保護された著作の許されない使用

(1) 法律上許容された場合を除いて、権利者の同意なしにその著作または著作の翻案もしくは改変を複製し、頒布しあるいは公然と上演した者は、3 年以下の自由刑または罰金に処する。

(2) 未遂は可罰的である。

この規定は、コンピュータプログラムの許容されない複製に対抗するために、著作権法に挿入されている。しかしながら、この犯罪構成要件の実現のためには、コンピュータプログラムの複製、頒布あるいは公然と再生することが必要である。
このような所為行為は、ウイルス攻撃における事案ではほとんど存在していないが、しかし、完全を期すために著作権法 106 条に言及したものである。

6. 行政法
ウイルス発生の場合の秩序監督局(Ordnungsbehörde)の処分として、秩序監督局法 14 条による秩序維持処分を考えることができる。これによると、権限ある秩序監督局は、公的な安全または秩序に対する危険が存在するかぎり、介入する権限をもつ。公的な安全の領域には、とりわけすべての実定法（もちろん刑法も）および個人の法益が属する。これらの法益に対する危険が存在するかぎり、当局は妨害者に対して行動をとることができる。ウイルスを作成したハッカーは少なくともこれにあたる。
妨害者に対する介入が可能でない場合にかぎり、当局は、現実の物的な支配の所有者にも、すなわちシステムへのアクセスを有する人物? いわゆる管轄妨害者ないしは非妨害者？にも一定の行為を命ずることができる。緊急の事案が存在するといえるならば、警察も必要な行為をおこなう権限を有する。

質問書に述べられている特定の責任についてのまとめ
(a) ソフトウエアまたはハードウエアの欠陥について製造者または開発者の責任（すでに利用されているプログラムの事後的な修正に利用されるパッチ、部分的なプログラムも含む）
ソフトウエアの製造者もしくは開発者は、典型的には、契約に基づいて責任を負う。標準的なソフトウエアを引き渡す場合には、売買契約が問題となる。売買の目的物に瑕疵がある場合、買主は、民法437条にあげられている諸権利を行使することができる。
そのためには、売主が義務違反をおこなっていなければならず、これを回避しなければならないことが必要であるが、この回避義務は故意・過失を意味している。売主が買主に対して当該物を瑕疵がないように調達しなかったという点に、義務違反が存在する。

さらに、上記で説明した製造物責任の諸原則または製造物責任法による責任を考えることになる。

(b) 情報セキュリティに対する攻撃の最初の被害者の責任、すなわちさらなる攻撃を阻止することを懈怠したことが、自己の管理するシステムが他の被害者のシステムに損害を与えることにいたった者の責任（公開されたパッチの適用義務や公知の脆弱性を無防備にしておかない義務を含む）
最初の被害者の刑法上の責任は故意がないために阻却される。過失は、すでに述べたように法律で規定されている場合にのみ可罰的であり、したがってこの場合には問題にならない。
契約を基礎とする責任も、両方の被害者には契約関係が存在しないから、ここで述べられている事例では否定されるべきである。

しかしながら、最初の被害者の不法行為に基づく責任は考慮される。民法823条 1項による責任の前提要件は財産の侵害である。第二の被害者のシステムが使用不能にされたことから、これは存在する。
この侵害は請求相手の行為によって生じなければならない。しかしながら、本件の場合、最初の被害者は積極的に行為してはおらず、ウイルスの他のシステムへのさらなる攻撃を阻止しなかったという不作為をおこなったものである。けれども、不作為が当罰的となるのは、社会生活上の安全義務をおっている場合だけである。すなわち対外的注意義務違反である。社会生活上の安全義務は不法行為の行動義務であり、義務の担い手が他人の法益に対する責任を引受けるということにいたる義務である。

それゆえ、ここで問題となっている事例では、最初の被害者が補諸義務を侵害したかどうかを検討しなければならない。このことは、基本的に、最初の被害者がウイルスについてどのような知見を備えていたか、および、どの程度彼にセキュリティ措置を講じることを期待することができるのかということに依拠している。

しかし、民法823条1項による最初の被害者の責任は十分ありうる。たとえば、最初の被害者が不十分なセキュリティシステムを理由としてウイルスの拡散、したがってより大きな危険源の放置について責任があるという場合ついて可能である。このような状況では、保証義務、したがって、継続的に行為する義務をも認めることができる。最初の被害者がこの作為義務を果たさないかぎり、民法823条1項の責任を負う。

(c) システムの脆弱性の効果的なセキュリティ監査を怠ったことについての責任

システムの脆弱性の監査に関する契約が当事者間に存在するかぎり、システムの脆弱性の効果的な監査を明示することを怠った者は、契約に基づき責任を負う。この場合、義務違反が存在する。それ以外の場合は、前述のことが妥当し、その際前提となるのは、監査をする者がシステムの脆弱性の監査を引受けることによって社会生活上の安全義務を負うということである。

ハンブルクラント裁判所の2001年7月18日の確定力ある判決(Aktenzeichen 401 O 63 /00) によると、データメディアをウイルス感染の検査を契約により引受けた会社は、最新でない検査プログラム使用したことによって検査の際にウイルスを見逃した場合に生じた損害について責任を負う。

3.2.2 法律上の責任のセキュリティの要素

情報セキュリティ、機密性、正確性ないしは可用性と法律上の責任との間にどのような関係があるか。

訴訟を起こすかぎり、企業は、その手続の範囲において、その現存のソフトウエアシステムについての機密性のある秘密情報を明らかにすることが必要となる。

裁判所に対する手続では提示の原則が存在する。当事者だけが、論争の素材を訴訟に導入し、その認定の必要性について判断し、その認定に従事することができる。裁判所は、当事者によって提出されなかった事実を判決において考慮することは許されない。

訴えの提起に関しては、実質的な訴えの申述が必要であり、訴えはそれ自体から容易に理解できかつ検証可能でなければならない。このことは、原告が訴訟にとって重要な情報をすべて開示しなければならないことを含んでいる。

それゆえ、ある企業がハッカーあるいはその他の者に対して請求を主張しようとするかぎり、どのようにウイルスの感染にいたりえたのか、また実際にはどのようになっているのかを原則として明らかにしなければならない。

この場合、訴訟は原則として公開であり、誰もが特に困難もなく、いつ、どこで裁判所が口頭弁論を開催するのかについて知る可能性を有している。しかしながら、録音と録画は許されていない。

重要な取引上もしくは営業上の秘密に関係するかぎりで、非公開にすることも可能である。

以上のこととは別に、当事者をのぞいて、第三者が、法的な利益を疎明することができる場合にかぎり、書類の閲覧のみ要求できる。

したがって、第三者は、ウイルスによって被害を受けた当事者のシステムに関する知識を獲得することができるが、しかし、原告がこのことを阻止しようとするかぎりで、非公開にする可能性も存在している。

3.2.3 主体的側面

情報セキュリティの侵害もしくはその未遂があった場合、被害を受けた当事者によって提起された訴訟において被告となりうる者はどのようなものか。

? ハッカー

攻撃者は、故意に損害を惹起した場合、刑法規範により責任がある。さらに、被害者は不法行為による請求を主張することができる。
ハッカーと被害者との間の契約は、圧倒的多数の事案で存在しておらず、そのため契約上の保証条項は排除される。
当該請求が成功する可能性は、たいていもちろん困難である。というのは、攻撃者がわからないかまたは連絡できないからである。

? 製造者あるいは開発者
典型的には、製造者または開発者は、被害者と締結した契約により責任を負う。そのほかにも、この場合、民法 823 条による製造者責任および製造物責任法による製造物責任が適用されるべきである。

? コンサルタント、システムインテグレーター、配布者、販売業者、あるいは欠陥のある技術を推奨しまたは指図したその他ベンダー（場合によっては、製造物の製造者との内部的な関係における連帯債務による責任）
標準的なソフトウエア販売業者の場合、製造者から発したコンピュータプログラムを故意にウイルスによって感染させないということが前提となる。
販売業者がソフトウエア製造業者によって販売用に完成して引き渡されたパッケージを独自に製造的な作業をせずにさらに販売するという場合がよくある。売主として、販売業者は、顧客に損害が生じないようにする付随的義務を有している。この限度で、故意もしくは過失で行為した（上記 3.2.1 参照）（中間）販売業者も、コンピュータウイルスによって惹起された損害について責任を負う。しかしながら、そのような者は、前段階の供給者、たとえばプログラムの製造者に賠償させることができ、支払った損害賠償を求償することができる。

しかも、製造業者を確定することができない場合。製造物責任法 4 条 3 項により、供給者を製造物責任法による製造業者とみなす。このことにより、ユーザは、製造業者がわからないために、自己の請求を達することができないという事態から保護される。
供給者は、当該請求が到達した後一ヶ月以内に被害者に製造者または先行供給者を知らせた場合、以上の代替責任を免れることができる。

OEM 販売業者は、これに対して、ソフトウエア製造業者からマスターデータメディア受取り、そこから複製製品を製造し、それを販売する権限を有している。その種の複製過程もしくは複製過程の直前の最終テストの段階でコンピュータウイルスに感染してしまうことはありうることである。この種の事案では、OEM 販売業者が、その製造監視義務を遵守しなかった場合、過失により行為している（民法 823 条 1 項）。その限度で、先行供給者、たとえばプログラム製造業者に損害を払わせることはできない。これらの者はウイルスの感染について責任がないからである。

? セキュリティの脆弱性の評価および回避を委任されたコンサルタント
すでに上記の3.2.1(c)で説明した、2001 年 7 月 18 日のハンブルクラント裁判所の判決が参考になる。データメディアをウイルス発生について検査することを契約によって引受けた会社は、検査の際に、最新ではない検査プログラムを使用することによってウイルスを見逃した場合、発生した損害について責任を負う。

? インターネットサービスプロバイダ
インターネットサービスプロバイダの場合、通常、プロバイダとコンテンツ提供者との間には記憶領域の提供に関して契約が存在している。サービスプロバイダが用意された他人のコンテンツに関して

予防的な監督義務にどの程度服するのか、したがって、ウイルスの発生が存在しないことを一定の事情のもとでもしくは通常確証する義務があるのかどうかが問題となる。

自らのところに蔵置され用意されているコンテンツに関する検査義務は、原則として、サービスプロバイダに課すべきではない。契約の相手方が適法に行動することを前提にすることが許されなければならない。
しかしながら、サービスプロバイダが具体的な法侵害を理由とする指摘あるいはそれどころか警告を受け取った場合は、積極的な認識をもったこの時点から服すべきことになる。この場合、遮断することも技術的に期待可能であるといってよい。テレサービス法 11 条により、プロバイダは、認識がある場合、遅滞なく活動しなければならない。

もちろん、期待可能性に関しては、サービスプロバイダの、その契約の相手方に対する特別の契約上の義務をも考慮されるべきであることありうる。権限なく切断する場合。サービスプロバイダは、今度は顧客にそのプロバイダ義務の違反を理由に責任を負うリスクに直面する。したがって、プロバイダには、契約相手と連絡をとることができる適切な対応時間が認められるべきである。この対応時間がどのくらいの長さであるのかは、個別の事案の問題であり、おそらくウイルスによって生じる損害を考慮しながら衡量されなければならない。

しかしながら、プロバイダが認識している場合にのみ責任を負うという上述の責任の恩恵は、提供しているサービスが機能可能性および安全性に関してその固有の保証義務を軽減するものではない。

サービスプロバイダが情報の伝送をそもそも誘因となっていないかぎり、テレサービス法 9 条 1 項により責任はない。
TDG による責任の免除は、刑法、損害賠償法および行政法の領域について妥当する。一般的な表現およびこのサービスの促進という点に存するこの規範の目的に基づくと、コンピュータウイルスも「情報」の概念に該当するということを前提にすべきである。

? 脆弱性を認識したが、これを報告しなかった当事者
ある当事者が報告を怠ったことについて責任を負うのは、そのような報告をおこなうことを義務を負っている場合のみである。このような義務は、契約関係の存在または一般的な保証義務のいずれかから導き出すことができる。
後者の義務を認めることができるのは、監督ないし監視義務を引受けていた場合だけであるが、しかし、なんらかの形態での危険源についても責任がある。

3.2.4 脆弱性の場所
1 どの場所に責任に関係する当事者が存在するかということが重要であるか。

? クライアント
? サーバ
? ネットワーク設備

原則として、被害の場所は損害賠償義務について重要ではない。もちろん、保護義務の程度は、個々のクライアントにおけるよりもネットワークにおけるほうがより高度となりうる。ネットワークを設置しているかぎり、責任ある当事者は、セキュリティの防護措置が場合によって付随的に強化されることがおこるはずであるということを意識しなければならない。

2 ソフトウエアを提供する態様が責任の射程範囲に影響をおよぼすか。

? エンドユーザのために販売されるソフトウエアパッケージ

? 個別開発ソフトウエア
? 外注
? 委託
? 特定のサービスを提供することに利用されるソフトウエア

ソフトウエアを提供する態様は契約類型を決める際に重要となる。したがって、どの保証条項が適用可能となるかという問題についても重要な役割を果たす。この場合にも、供給者に対するどのような要求を認めるべきかは、それぞれ異なって検討されるべきである。

3.2.5 注意義務? 標準
3.2.5.1 一般
1 法規が注意義務の標準を情報セキュリティの保護の場合に差異をもうけているか。
2 ソフトウエアのセキュリティの欠如またはその他の脆弱性を改善する義務に関して基準が存在するか。
3 私人についてもそのような基準が存在するか。

具体的な技術的なセキュリティの基準をもつ法令あるいは技術上の規格に対する参照は現在ドイツには存在しない。

ソフトウエア産業にその保持を義務づける詳細にわたった法律上の状態に関する指図を設けることも、ほとんど期待することはできない。その種の具体的な基準を異なったハードウエアプラットフォームに関して、かつ、様々な利用されるプログラミング言語、エンジニアリングの方法および品質保証手続に関して詳細に表現することはほとんど可能でないように思われるということは別として、その種の法律上の明文化は望ましくない。法的明確性というこれと関連するメリットは、その種の明文化が拘束力のある状態に関する指図によってコンピュータ技術の領域における技術的な進歩の急速な展開を阻害することになるというデメリットがうわまわっている。

製造業者によって保証義務の枠内で期待されることは、その製造物の取引の安全を保証するということである。この取引の安全が存在するかどうかは、連邦通常裁判所の判例によると、技術的な基準によって判断される(BGH 92, 143, 146)。その場合、製造業者の注意義務に対する要求は危険の程度と損害発生の可能性によって高まることになる。

情報技術における安全性に関する連邦庁(BSI)の、この関連において作成された「情報技術のシステムのセキュリティ監査に関する基準」は、システムのデータの機密性、完全性および可用性を保証するためのセキュリティ基準を内容としている。しかしながら、これを参照することで、この基準は、そのセキュリティ基準を保証すべきプログラミング方法にも影響をおよぼしている。

人的なデータを処理する機関については連邦データ保護法 9 条が妥当する。

連邦データ保護法 9条 技術的かつ組織的な処理
自らまたは委託して個人に関するデータを発生させ、処理しあるいは利用する公的ならびに非公的な機関は、この法律の諸規定の実行、とりわけこの法律の序文で述べられている要求を保障するために必要である技術的ならびに組織的な処理をおこなわなければならない。その費用が達成しようと努められる保護目的に対して適切に対応している場合にのみ、処理は必要である。

したがって、この規範の名宛人には、たしかに、個々の事案に適合されたデータセキュリティの措置をおこなう可能性を開くものではあるが、しかし、同時に、複数の可能な防護措置のどれが必要であるかという判断もしなければならない。
個々の連邦のデータ保護の受託者は、これらの要求をさらにさらに充足して、勧告を与えるのである。

3.2.5.2 管理者の義務
１ 脆弱性を修正することができるパッチやソフトウエアを投入するようにという実際の指示があったにもかかわらず、これを怠ったシステム管理者は責任を負うか。
２ システム管理者が、セキュリティ情報を収集しなかった場合、責任を負うか。

責任の可能性に対する質問については、システム管理者の作業に関する契約がどのような種類が選択されていたかが区別されるべきである。
一方では請負契約(Werkvertrag)として、他方では雇用契約(Dienstvertrag)として位置づけることが可能である。どの契約類型に該当するかということは、指示のその他の事情に依拠している。完成した最終製品の責任があるかぎり（有効なパッチをもったシステム）、請負契約が存在し、一定の作業の結果の責任を持つことなく労働作業それ自体の責任があるといえる場合は、雇用契約が認められるべきである。
義務の内容は個々の契約の取り決めにより確定される。請負契約であっても雇用契約であっても、いずれの場合にも、管理者は有効なパッチを投入するように指示を受ける。

服務義務のある者がその能力の欠如を主張しなければならない場合、あるいは、その義務を有責に不十分に充足した場合、雇用権者は民法 280 条により損害賠償を要求することができる。
服務義務のある者が労働関係にあるかぎり、損害賠償の請求は経営上させられた活動の原則より場合により減額することが可能である。これによると、被雇用者は、故意または重大な過失の責任がある場合にのみ完全な責任を負う。通常の過失の場合、損害は雇用主と被雇用者との間按分されることになる。このように損害を配分する場合、具体的事案の状況、とりわけ被雇用者の企業への帰属の継続性、その報酬の額および損害の程度が考慮されるべきである。

請負契約が認められるかぎり、望まれるパッチをあてないシステムは瑕疵があるものとみなされるべきである。この場合にも、注文主には損害賠償請求が民法 634 条、280 条により認められる。

さらに、契約上の責任とは別に、民法 823 条１項、2 項によりシステム管理者の責任が存在することがある。

3.2.5.3 インシデントの際のシステム管理者の義務
１ インシデントに対応する場合、システム管理者は以下の点に責任を負うか。
? 不十分な対応
? 遅すぎる対応
原則として、インシデントが発生した場合、義務違反の責任を負いうる当事者の責任がすでに生じている。場合により、この損害賠償義務のある者は、管理者が請負契約による義務に違反し、そのことによって損害を増加させた場合、管理者に賠償を負担させることができる。このことはもちろん管理者の有責性の問題である。

専門的なシステム管理者もウイルスの発生によって大きな問題に直面し、その高度の専門能力にもかかわらず、その問題をつねに解消するとはいえないということは、明らかとなっている。少なくとももっとも重要なセキュリティにかかわる領域で技術の水準にとどまるために払わなければならない経費は実際法外なものである。プログラムのバージョンの速やかな変更とハッカーによる新しいバージョンにおける脆弱性のかろうじてより早い発見は、適切な情報源をつねに観察することによって達成する。この場合、一般的に新規ニュースはまっさきにインターネットの雑種雑多なフォーラムで公表されるということを前提にすることができる。それゆえ、管理者は、製造者やサービスパートナーによって適時に情報を与えてもらえることを信頼することはできない。
したがって、当該管理者に故意または過失があるといえるかどうかは、つねに個々の事案における具体的な衡量の問題である。

それ以上に、管理者の責任に関しては、ここでも再び、企業上必要な活動の原則が適用されるべきであり、このことによってその責任が軽減されうる。

2 損害を軽減する責任を有している当事者は存在するか。
被害者についても、法律上の損害回避義務が存在する。
被害者が損害を軽減する義務を怠った限度で、民法254条2項が関係することになる。被害者が損害の回避もしくはその軽減に十分な程度に寄与しなかった場合、損害賠償請求はそれに応じて減額される。

被害者が損害について共同して責任があり、もしくはこれを減少させなかったという事情は、すでに述べたように(3.2.1 契約法参照)、その額の減少にいたる。判例は、その場合、様々な技術的な可能性（データの保全、ウイルスの検査）と行動準則を遵守しなかった場合、損害が発生したときでも、共同責任があると判断している。

3.2.5.4 セキュリティポリシー
1 法律は注意義務の規準の一部としてセキュリティポリシーを要求しているか。
情報セキュリティにおける注意義務の規準について詳細な法律上の規定は存在しないことから、一般的な責任の規範が独自の具体的なセキュリティポリシーの作成を要求することになる。あらゆる製造業者、開発者、供給者などは、必要な注意義務の規準を充足するために、そのソフトウエアをその技術の現在の基準に適合させるよう強制させる。

EU 委員会は、さらに言及されるべきセキュリティポリシーとして、情報システムに対する攻撃に関する2002年4月19日の議会の基本決議に関する提案を可決した。提案された?技術的に中立の?決議は、EUにおける刑法の諸規定を比較することによって刑事訴追当局ならびに司法当局に情報システムに対する犯罪の最新のもっとも重大な形態に対する効果的な対策を可能にすることをめざしている。それは、「ネットと情報の安全性：ヨーロッパの政策アプローチに対する提案」というその報告において委員会によってあげられた、情報システムへの違法なアクセス（ハッキング）とたとえばサービス妨害や有害なソフトウエア（ウイルス）の頒布という形態での情報システムにおける違法な侵害という攻撃の可能性、ならびに、通信の傍受におよびユーザの詐欺と欺罔を批判している。なかでも2002eEuropeという行動計画は決議の枠組みを形成している。

2 たとえば保険会社や事業者協会のように、導入されている私的なガイドラインや標準は存在するか。
契約の次元では、ソフトウエアの発注者と受注者により、ソフトウエアが最新の品質補償基準により開発されるということが一層強力な程度に期待される。この期待は、コンピュータプログラムの多くの製造業者がその製品を品質保証システムに関する認証機関、たとえばドイツ品質保証協会(DQS)、DEKRA あるいはTÜB によって認証させるという点にも映し出されている。

BSI は、昨年、IT安全性基準を公開した。これは、安全で信頼できるシステムを開発するための基本方針として役立ち、当該システムを中立的で能力のある機関による客観的な評価を可能にし、ユーザに適切な IT 安全性のある製品を選択する可能性をあたえるものといえる。この基準を基礎にして、情報技術の製品とシステムを認証する可能性が生じる。現行の安全性基準は以下のサイトを通じてリードバックできる。
<http://www.bsi.de/zertifiz/itkrit/itkrit.htm>

さらに、2002年5月にはBSIのIT基本保護ハンドブックが公刊され、その都度最新の基準が維持されている（現在は2003年5月）。官庁の周辺でも、私的な経済領域でも、企業は、IT基本保護ハンドブックをセキュリティ措置の標準の構想、現実化および再検討に際しての補助手段として使用している。
IT 基本保護ハンドブックは以下にダウンロードできるように用意されている。
<http://www.bsi.de/gshb/deutsch/menue.htm>

インターネットセキュリティというテーマについても、BSIのホームページには、様々な研究、公報および文書が存在している。これらは以下で閲覧可能である。
<http://www.bsi.de/fachtem/sinet/index.htm>

ヨーロッパの次元では、「情報技術セキュリティ評価基準? ITSEC」が1998年3月3日に施行されている。ここでは、情報技術の安全性を評価するための基準がまとめられている。
ITSECは以下で閲覧できる。
<http://www.bsi.bund.de/zertifiz/itkrit/itsec-en.pdf>

3 セキュリティポリシーを実行することが責任負担を阻止する「セーフ・ハーバー」を形成するか。
品質のメルクマールについては一致があるにもかかわらず、品質のメルクマールが最適化されて達成され、プログラミングの際に具体的に実現されることが可能である基準を統一しているということはない。品質の規定はあまりに不明確なままであり、もっぱらその内部で品質保証をおこなわなければならない枠組みを述べているにすぎない。それぞれのソフトウエアの欠陥のない開発プロセスに対する明確な指示はそこからは明らかにならない。
それゆえ、個別の詳細はセキュリティポリシーを展開することに依拠することはできず、たえずセキュリティポリシーに設定された要求をアップデートしなければならない。

4 セキュリティの監査およびセキュリティの評価を実施することが、セキュリティの監査および評価が発見しなかった脆弱性に対する責任を軽減する「セーフ・ハーバー」となるか。
一般的な品質基準を維持するかぎり、私法上、有責性を認めるべきではない。一般的なセキュリティ基準が通常アップデートされ、検証されている場合、ウイルスの発症に関して有責性を認めることはできず、そのため責任が阻却される。
周知の方法によって検地されず、したがって阻止することもできなかった新種のウイルスについては、ソフトウエア開発者あるいは製造業者に責任を問うことはできない。
したがって、この局面のもとでは、通常の、かつ技術の最新の基準を維持したセキュリティ監査を実行することは「セーフ・ハーバー」となる。

3.2.6 その他
1 セキュリティ・インシデントの実体を明らかにするように規定する法的システムは存在するか。
この点に関して特別の法令等は存在しない。しかしながら、作為義務は契約または不法行為により生じうる。このことについては上記で説明したことを参照のこと。

2 情報提供者の保護のシステムまたは自白の場合の刑の量定手続に関する法律を有しているか。
裁判所手続法172条1項a号によると、証人もしくはその他の者の保護のために、公判を非公開にすることができる。
証人の健康にとって重大な損失となる切迫した危険が存在している場合、裁判所は、刑事訴訟法247条aにしたがい、証人を公判中別の場所へとどめておくことを指示することができる。この場合、その証言は映像と音声で同時に公判廷へ伝送される。
刑訴法68条によると、証人に対する危険が現存する場合、個人的なことにかかわる供述をする義務を制限することができる。

刑法においては、有罪判決をするためには、原則として構成要件が立証されなければならない。このことは、被告人の自白によってもなしうる。そのような自白は、刑の減軽事由となりうる。

3 上述のこととセキュリティポリシー・インシデントの解明との関係に関する議論は存在するか。

この点に関して議論が見受けられない。

3.3 開示義務
１ ソフトウエアまたはハードウエアの脆弱性を知ったとき、これを会社もしくは公的機関に報告する法律上の義務は存在するか。
労働関係がある場合にも、両当事者の、他方の権理、法益および正当な利益を配慮する義務は存在する。このことの法的基礎は民法 241 条 2 項、242 条と関連している労務契約(Arbeitsvertrag)である。

特別の付随義務として、従業員は、労務契約および雇用主の指示により概要が示されるその活動範囲において発生しあるいは切迫している損害をともかく雇用主に報告しなければならない。
どの程度従業員がその活動範囲の外で損害が切迫していることを届け出ることを義務づけられているかということは、所与の個別の事案の事情に基づき具体的な利益考量を基礎としてのみ判断することができる。

3 産業界や政府の機関によって提案された、違反を知ったときにこれを開示する義務についてのなんらかのガイドラインは存在するか。
4 開示された脆弱性を評価することを専門家委員会に義務づけているか。
この点についてはわからない。

3.4 SQL Slammer
SQL 事件以降、この種のインシデントを回避するための議論は存在しているか。
2003 年 1 月の SQL Slammer ワームあるいは2002 年の DNS ルートサーバに対する攻撃のようなセキュリティのインシデントが示したことは、IT セキュリティは引続き積極的に推し進められなければならないということである。すでに述べた連邦政府のセキュリティ・イニシアティブ、たとえば「安全なインターネット」や「安全なインターネット産業のパートナーシップ」というタスクフォースとならんで、BSI は、今年、インターネットにおけるセキュリティを実行に移す場合にとくに市民を支援することになるイニシアティブをスタートさせた。
www.bsi-fuer-buerger.de というウエッブアドレスのもとでは、インターネットの安全な利用をめぐるすべてのテーマについてのわかりやすくて実行しやすい情報が入手できる。補充的に、このウエッブサイトを通じて、BSI によってまとめられたセキュリティツールを無償でダウンロードすることができる。このようにして、インターネットをより安全に利用することができるようにするために、特にインターネットの参加者にとって有益な示唆やツールが供与されている。それ以上に、BSI における CERT は他の CERT と国家的な CERT 連合の枠内で共同活動を強化することを取り決めている。こうして、従来より一層改善されて損害の事案に対して将来対応することができるために、相乗効果の可能性がある。

3.5 脆弱性がある場合の適切な行動ためのガイドラインについて情報を提供してください。
これについては上記に述べたことを参照のこと。

（余白）

『セキュリティホールに関する法律の諸外国調査』報告書

付録　B－6

大韓民国　報告書日本語訳

（余白）

情報セキュリティ比較調査研究　質問事項に対する回答

（大韓民国　㈱ローアンドビー　代表取締役／弁護士　李　海完）

下記の質問事項に対する韓国の法規、判例、学説、その他の情報を参考に次のように回答いたします。

III.　質問事項(The Questions)

以下においては、「法」という用語を、この質問票に関するかぎり、制定法、規則、法令、判決例、行政規則などのすべての公の準則をいうものとする。

3.1 定義(Definition)

3.1.1.脆弱性を議論するにあたって、「ソフトウエア」の定義が法にありますか。[IT1]

【回答】脆弱性と関連した脈絡に限定されるものではないが、「ソフトウェア」の定義を規定した法条文がある。ソフトウェア産業振興法第２条第 1 号において「『ソフトウェア』というのはコンピュータ・通信・自動化などの装備とその周辺装置に対して、命令・制御・入力・処理・保存・出力・相互作用が可能になるようにする指示・命令（音声または映像情報などを含む）の集合と、これを作成するために使用された技術書その他関連資料をいう。」と定義しているのがそれである。これが韓国の法律上ソフトウェアの定義を下している唯一の規定だと判断する。ソフトウェアと類似した概念としてコンピュータプログラムという用語があるが、これに関しては著作権法　第２条第１２号にて「コンピュータプログラム：特定の結果を得るためにコンピュータ等の情報処理能力を持つ装置内で直接または間接的に使用される一連の指示・命令によって表現されたものをいう。」と定義規定をおいてあり、コンピュータプログラム法第２条第１号において、コンピュータプログラム著作物に対して、「『コンピュータプログラム著作物』とは、特定の結果を得るためにコンピュータなど情報処理能力を持つ装置（以下「コンピュータ」という）内で直接または間接に使用される一連の指示・命令で表現された創造物をいう」と定義規定をおいている。著作権法とコンピュータプログラム保護法にて定義されたコンピュータプログラムは、著作権法上、著作物の一つとして取り扱われている文脈でコンピュータプログラムを定義した規定だ。ここで定義されたコンピュータプログラムの意味をソフトウェア産業振興法によって定義された「ソフトウェア」の意味と比較してみると、ソフトウェアの意味がプログラムに比べて「・・・これ（*プログラム）を作成するために使用された技術書その他関連資料」を含めているという意味で、その分もっと広い概念であることが分かる。

3.1.2.「セキュリティホール」「脆弱性」「不具合」について法令等で定義をしていますか。[IT2]

【回答】韓国法で法令用語に外国語を直接使用している例が増えているが、原則的に

は韓国語に換えて表現するよう努力している。そこで、「Security　Hole」も韓国法では「脆弱点」という韓国語に換えて使用している（即ち、韓国法で使用している脆弱点という用語は、「security hole」と同じ意味と判断されている）。ただし、これに対する定義規定を法に定めてはいない。‘ 脆弱点 ’という用語を使用している法令は２００１年１月２６日に制定された法律である「情報通信基盤保護法」（２００２年１２月１８日一部改正）とその施行令である（添付資料＃1、＃2参照）。一方、「情報通信網利用促進ならびに情報保護に関する法律」に基づいて情報通信部長官が制定し公示した「情報通信サービス情報保護指針」第８条において「保安脆弱点」という用語を使用しているが、同じような意味の用語であるといえる（添付資料＃８参照）。

情報保護と関連して一般的な事項は、「情報通信網利用促進ならびに情報保護に関する法律」において規定しており、特に国家的・社会的重要性を持つ重要情報通信基盤施設をサイバーテロ攻撃などから保護する問題に対しては、「情報通信基盤保護法」で規定している。

「欠陥」という用語は、「脆弱点」とは多少異なる概念として一般製造物の欠陥に起因した製造物責任と関連して使用される用語で、製造物責任法において、その定義規定を置いてある。即ち、製造物責任法第２条にて、「『欠陥』というのは、当該製造物について、次の各項目のひとつに該当する製造・設計または表示上の欠陥、もしくは、その他通常、期待できる安全性が欠けているということをいう。」と定義している。

3.1.3.「セキュリティ・ホール」という用語が法令等で使用されていませんか。

【回答】上記の質問に対する回答を参照。

3.2. 責任(Liabilities)

3.2.1　一般的フレームワーク(General frame work)

情報セキュリティの脆弱性もしくは不具合による責任について、定義や責任が定められていますか。[IT3]

【回答】特別に対象を限定して、情報セキュリティの脆弱性と関連した責任にまたは、ソフトウェアの欠陥に対する責任に関して特別に民事責任要件等を規定した法令はない。「情報通信網利用促進ならびに情報保護に関する法律」および「情報通信基盤施設保護法」上のいくつか義務規定が、民事責任の一つの要素である過失の有無の判断に対して一つの基準になり得るだけである（このような規定の詳細な内容は、後で該当する質問へ答えながら紹介していく）。結局、民事責任の有無と損害賠償の範囲等を決めるに当たって、民法上の不法行為、債務不履行、製造物責任法上の製造物責任等に該当するか否かを検討することとなる。

もし、必要であれば、請求原因を不法行為、制定法、契約法に分けることもかまいません。

【回答】以下で、民事責任の類型を不法行為、債務不履行、製造物責任の三つに分けて、一般的フレームワークに関する説明をする。

民事上の責任について詳細に記述してください。ただし、脆弱性の濫用に対しての刑事

的責任[IT4]および行政的手法についても概観してください。

【回答】下記では、刑事責任と行政的な事項に対して別途説明をすることとする。

以下の責任についての論点を考慮にいれて報告ください。

(a) ソフトウエアまたはハードウエアに欠陥があった製造者 ,開発者の責任
(b) 「下流責任」[IT5] (情報セキュリティに対する侵害攻撃を停止するのに失敗した最初の被害者の責任、すなわち、そのシステムが他者のシステムを攻撃するのに利用された責任 -公開されたパッチを宛てるのを怠った責任や公知の脆弱性に対応するのを怠った責任)
(c) システムにおける脆弱性を発見するために効果的な監査を怠った際の責任

【回答】上記の問題に対しても下記で一緒に述べることとする。

【回答】情報セキュリティに関する責任の一般的フレームワーク
１．民事責任

上で回答したように民事上責任を問う請求原因を、不法行為、債務不履行、製造物責任の三つの類型に分けて報告する。

（１）不法行為

韓国で不法行為は、一般不法行為と特別不法行為に分けられる。一般不法行為とは、不法行為に関する基本的な条項である民法第７５０条（故意または過失による違法行為により他人に損害を与えた者は、その損害を賠償する責任がある）の規定による不法行為をいい、特別不法行為とは民法第７５０条に対して特則を定めた特別法に基づく不法行為をいう。
自動車損害賠償保障法において、無過失責任として取り扱っている自動車事故などの場合がこれに該当し、後で述べる製造物責任もこれに該当するといえる。
韓国法上、ＩＴの領域にも不法行為と関連した特則規定が、何箇所かで規定されている。その中の一つが個人情報の侵害に関連して、侵害者の故意、過失に対する立証責任を転換した「情報通信網利用促進ならびに情報保護に関する法律」第３２条の規定［利用者は、情報通信サービス提供者などのこの章の規定に違反した行為により損害を受けた場合には、その情報通信サービス提供者などに対して損害賠償を請求できる。この場合、当該情報通信サービス提供者などは故意または過失がないことを立証しなければ責任を免れることはできない。］であり、もう一つは電子署名と関連した公の認証機関の責任を重くする電子署名法第２６条の規定［公の認証機関は認証業務遂行と関連して、加入者または公の認証書を信頼した利用者に損害を与えた場合は、その損害を賠償しなければならない。但し、その損害が不可抗力により発生した場合は、その賠償責任が軽減され、公の認証機関が過失の無いことを立証した場合には、その賠償責任は免除される。］

である。

しかし、まだ本事案と類似した情報セキュリティに関連する問題に対して、民法第７５０条に対する特側によって不法行為に関する規定は置いていないので、結局この問題は、一般不法行為の原則により解決されることになる。

一般不法行為の成立要件は、１）故意又は過失、２）違法性、３）責任能力、４）損害の発生など 4つである。この中で主に問題になるのは１）と２）である。

その中でも故意または過失が特に重要な要件であり、故意というのは、「自己の行為により一定の結果が発生するであろうと認識しながら、その結果の発生を容認して敢えてその行為を行うという心理状態」を意味しており、過失とは、「ある行為により一定の結果が発生することを知り得たにも関わらず、それを知らないで行ったという場合」に認定されるものである。過失では、その概念的前提として、注意義務があり、この注意義務違反が過失になる。

ところで、過失に関しては、その前提となる注意義務の種類によって、抽象的過失と具体的な過失の区別がある。抽象的過失とは、「善良な管理者の注意」が欠けた過失で、具体的な過失とは、「自己資産と同一の注意」が欠けた過失である。不法行為における過失とは、その中の「抽象的な過失」をいう。

それは一方では、通常人として行わなければならない注意をしていれば足りるし、その場合、もっと周到綿密な注意をしていれば損害の発生を防止できたとしても過失はない。しかし、それはもう一方では、注意力が足りない者であっても、通常人として行うべき注意を行わなかった場合には、過失があることになる。

しかし、抽象的な過失といっても、非常に抽象的、一般的に過失を考えることは適当ではない。例えば、自動車運転者については、運転者に通常必要となる注意義務が基準となることであり、それを離れて「通常人」を考えることは無意味である。

即ち、通常人というのは、その職業、地位における通常人を意味するのであり、過失の認定に関しては、その事件の性質や環境も当然、考慮することになる。一方、ある地位に対して、法により、ある作為義務または不作為義務を課する取り締まり規定を設けてあれば、それもその地位にいる人の注意義務を構成することになる。法に明示的な規定がなくとも、いわゆる社会常識または条理に照らして、特定の地位または立場にある人に、一定の注意義務があると認定する場合もある。ところで、このような部分は不法行為の成立要件中、違法性と連結され得るものである。

上記のような過失の概念を注意義務違反と見なす場合、その概念には事実上、違法性の概念も含めることになることが分かる。即ち、注意義務違反が認定されると過失と違法性が当時に認定され得るものであり、そのように取り扱って違法性を別途に検討しないで、注意義務違反の可否だけを検討するのが韓国の判例の立場である。これは日本の場合と違わない。

従って、実際の不法行為訴訟において１）注意義務が認定されること、２）その注意義務に違反したこと、３）損害が発生すること、４）損害発生と注意義務違反の間で相当の因果関係があること等の四つの要件を審査することになる。ここで基本的に重要なことは、注意義務の認定の可否である。本質問において問題になる事案を解決するにあたっても、その要諦は結局、注意義務が認定されるかどうかにある。

これに関連して、各責任主体別にどのような基準で判断しなければならないかに対しては、後の該当する質問に回答しながら詳細に言及することとし、ここでは、上記の質

問で提示されたいくつかの質問に対して回答することにする。

まず、（a）ソフトウェアまたはハードウェアに欠陥があった製造者、開発者の責任に対する問題を検討する。この問題は後で言及する製造物責任法に基づく製造物責任と関連してよくみかける問題でもある。しかし、製造物責任は一定の要件のもとで、民法第７５０条の一般不法行為規定に対する特側を規定したものなので、その特側規定の要件を充足していない場合は、再び民法第７５０条の一般不法行為の要件に該当しているかを検討することとなる。ソフトウェアの場合、製造物責任法の適用対象物である「製造物」に該当するかに対する疑問はあるが、ソフトウェアの欠陥に対しても一般不法行為の成立は完全に排除するものではないと考えられる。問題は、ソフトウェア製造者が社会常識上、このような欠陥のあるソフトウェアを市場に出さない注意義務があるといえるかどうかにある。それは具体的な事案ごとに、異なる結論が出る可能性がある問題であり、一律に断定してはならない。例えば、会計プログラムを作って市場に出したのに、そのプログラムの重大な欠陥により会計が不正確になって、購入者が被害を受けたら、場合によっては不法行為責任が認定され得るであろう。

不法行為責任と製造物責任のもっとも大きな違いは、加害者の故意過失を立証する必要があるか否かである。被害者が製造物の欠陥に対して不法行為責任を主張するのだとしたら、多くの場合、故意・過失の立証に苦労することになるであろう。それが製造物責任法の立法趣旨でもある。

次に(b)下流責任の問題について検討することにする。韓国で下流責任に関して別途の法規定があるわけではない。この問題も上で明らかにした「注意義務違反」があるか否かの観点から原論的に解決するしか他にない。即ち、情報セキュリティに対する侵害攻撃を停止することに失敗した最初の被害者の責任の有無を検討するに当たって、その人が被害者であるというのは、絶対的な意味を持ち得るのではない。その人自身が被害を受けたこととは関係なく、他の被害者たちとの関係で、自分が情報セキュリティに対する攻撃を予防したりシャットアウトしたりする処置を行う注意義務があったにも関わらず、これを履行しなかったことにより、被害を発生させたり拡大したりした場合であれば、不法行為責任を負わなければならない。この場合に重要なのは、その一次的被害者の地位、技術的な対処可能性、その他いろいろな事情に照らして、法令または社会常識上、注意義務があるといえるかどうかである。これも同じく、具体的な事案別に個別的な判断を下すべきで、一律に断定することはできないが、そのような注意義務の存在とその違反に基づいた損害発生が認定されて、不法行為責任を負う場合もあり得ることを排除することはできないであろう。以上の観点は、韓国の法令、判例に照らして大きな疑問があるものではないと考えられる。特に、公開されたパッチを設置することを怠った場合や、広く知られている脆弱性に対する適切な処置を行うことができるのに、そうしないことにより、多数人に被害を与える場合であれば、責任が認定できる可能性は多いと考えられる。

次に（C） システムにおける脆弱性を発見するため、効果的な監査を怠った場合の責任に対しては、上記の（ｂ）において言及し、明らかにした内容が基本的に適用される

ことになり、おそらくは、政府の責任と関連した問題に繋がるようであるが、その部分は後述の責任主体別の論議において再び言及することとする。

（２）債務不履行（契約責任）

債務不履行責任と関連して、韓国の民法第３９０条は、「債務者が債務の内容に従い履行を行わない場合には損害賠償を請求することができる。但し、債務者の故意や過失なしに履行できなくなった際にはこの限りでない。」と規定している。但書規定により、故意、過失のない場合は債務不履行責任を負わなくなるが、それが但書規定にあるため、立証責任は、故意、過失がなかったことを主張する債務者にあるものと解釈される。それが不法行為責任と大きく異なる部分である。

そして、不法行為責任は加害者と被害者の間で契約関係があるかの有無には関係なく、上記で説明した要件だけが充足されると認定され得るのに反して、債務不履行責任は原則的に損害賠償請求者とその相手の間の契約関係を前提としているという点に重大な要件上の違いがある。

例えば、ISP と PC 喫茶店業者またはインターネットショッピングモール業者などの間で、インターネット専用線サービス契約などが締結されていて、その専用線サービスが一時的に麻痺してしまった場合、一旦、債務不履行責任が問題になり得る。

その際、ISP が責任を免れるために、「ISP の故意、過失などの責任ある事由がなかった。」という点を積極的に立証しなければならない。不可抗力によることだという主張は、帰責事由を否定する主張の一例であるため、その立証責任は ISP にある。

上記で関連質問として提示された事項に対して、ここでも少し言及しておく。

(a)ソフトウェアまたはハードウェアに欠陥があった製造者、開発者の責任は、その製造者また開発者と被害者（一次被害者を含む）などの間で契約関係が存在しない限り、契約責任としての債務不履行責任は問題にならない。直接供給者として供給契約を結んでいたとしたら、供給契約の相手との間で瑕疵担保責任が問題になり得る。例えば ISP へ供給したハードウェアまたソフトウェアに欠陥（瑕疵）があったとしたら、韓国民法第５８条、第５７５条に従い、購入者側から損害賠償請求をするか、それによって契約目的を達成することができない場合には、契約解除をし得る権利がある。しかし、このような権利は購入者に限られ、他の二次、三次の被害者とは無関係である。その場合、不法行為責任また製造物責任が問題になる余地があるだけである。

次に、(b)下流責任の問題について見るならば、契約責任においても、情報セキュリティに対する侵害攻撃を停止することに失敗した最初の被害者が、自己の顧客に対して負担するインターネットの正常な運営と提供に関する債務の不履行について、その者が最初の被害者であるということだけで免責を主張することはできない。自分が受けたその被害は自己が注意義務を履行したとしても免れることができない「不可抗力」の事件であったことを立証した場合に限り、責任を免れることができる。それは即ち、その者が自己に故意、過失がないことを立証しなければならないという原則に対して、例外とはならないことを意味しているのである。

最後に、(c)システムにおいて脆弱性を発見する為、効果的な監査を怠った際の責任に対して見てみると、その監査義務を契約関係によって負担した場合であれば、契約責任（債務不履行責任）を負わなければならないし、そうではない場合は債務不履行責任の

問題ではないといえるであろう。

（3）製造物責任

韓国では２０００年に製造物責任法を改訂したが、その立法的背景と重要な内容は次の A～H の通りである（法律全文は添付資料#4 を参照)。本質問と関連した事項は I において言及する。

A．立法的背景

製造物責任(Product Liability, PL)とは、欠陥がある製品によって、消費者また第三者の身体上、財産上に損害が発生した場合、製造者、販売者など、その製造物の製造、販売の一連の過程に関与した者が負担すべきの損害賠償責任をいう。
製造物責任法が立法化された背景を考察して見ると次の通りである。
１９７０年代以降、産業社会の急激な発展、現代科学技術の高度化などで製造物の欠陥による事故が頻繁に発生した。その後、１９７７年に、製造物責任に関する問題解決のため、韓国民事司法学会において製造物責任を論議して以来、多くの研究結果が発表され、裁判所では、製造物責任の問題を、過失責任主義に基礎をおいた現行法の不法行為責任の枠内で解決しようとする試みがあった。
しかし､学会においては､現行法の解釈を通して製造物被害者の救済は不十分であり、外国においても製造物責任法の立法化傾向が進んでいることを理由として、国内消費者の保護と企業競争力の強化という目標を達成するため、製造物責任法制定の立法の必要性を提議することになった。
そして、２０００年1月２１日に公布され、２００２年 7月 1日に施行された法律第６１０９号製造物責任法が誕生することになった。
立法化された製造物責任法のもっとも大きな意義は、被害者の被害証明負担が軽減したことであり、これをはじめ、下記で、製造物責任法に特有の内容中、①製造物責任法の対象となる製品、②責任主体および、③製造物責任を問うことができる場合と、④損害賠償を受けうる被害の範囲、⑤製造者の免責事由ならびに責任期間の問題などを検証する。

B．製造物の概念

製造物責任法の対象になる製品は､「他の動産や不動産の一部を構成する場合を含んだ製造また加工された動産」である（製造物責任法第 2 条第 1 号)。従って、製造・加工ではなく、生産の対象と考えられる、一次農産物（林産物、蓄産物、水産物を含む）は本法の適用の対象にならない。また、機械・エアコン・ボイラーなど、それ自体の販売ではなく、器具の設置に瑕疵が有ったとしても、製造物責任法に基づいて責任を問うことはできない。
そして､「動産」の意味は、不動産を除外した全てのものをいい、一定の形態を持った個体・液体・気体のような有体物は勿論、形態がない電気とその他、管理し得る自然力も含まれている。但し、アパートやビルのような不動産それ自体は、本法の適用対象に

ならない。しかし、不動産の一部を構成しているとしても、照明施設、配管施設、空調施設など、個別的な動産は本法の適用対象に含まれる。

C．責任を問える場合

製品により事故が発生したとしても、無条件に製造業者の責任を認定するものではない。被害者は製品に欠陥があり、その欠陥により被害が発生した場合だけ製造業者に製造物責任を問うことができる。

製造物責任法上の「欠陥」とは、製造物の性質、使用方法などに対する説明、指示、警告その他の表示など、合理的に予想し得る当該製造物の使用形態、製造者などが当該製造物を流通させる時期など、あらゆる事情を考慮して、製造物に通常期待できる安全性が欠如することを意味する（製造物責任法第２条第２号）。

製造物責任において、欠陥はあくまでも製品の安全性に関する概念であるため、単純な製品の性能不足、品質不良のような、安全性に直接関わりがない、品質上や機能上の問題とは区分されている。

製造物責任を認定し得る製造物の欠陥は次のように分類できる。

①製造上の欠陥（製造物責任法第 2 条第 2 号ア目）

製造過程での不注意により、製品の設計仕様や製造方法に従わずに製品が製造されて安全性が欠如した場合をいい、このような欠陥は製品の製造、管理段階における人的・技術的不注意によるものである。例えば、品質管理の不良、安全装置故障、組み立て状態の検査不良、部品不良などが挙げられる。

②設計上の欠陥（製造物責任法第 2 条第 2 号イ目）

製造物の設計段階で安定性を十分に配慮しなかったため、製品の安全性が欠如した場合で、その設計により製造された製品は全て欠陥があるとみなすことができる。例えば、安全設計不良、安全装置不備、重要原材料および部品の不適合などが挙げられる。

③表示上の欠陥（製造物責任法第 2 条第 2 号ウ目）

消費者の使用または取扱い上、一定の注意を払わなかったり、もしくは不適当な使用をした場合などに発生し得る危険に備えて、適切な注意や警告を行わない場合をいうものであり、製造者はその製造物の使用から発生し得る危険に対して警告を行わなければならない。例えば、取扱説明書・警告事項の不備、表示不良（拡大・詐欺）、警告不適切などが挙げられる。

上記の三つの種類の欠陥を判断するにあたって、①危険の頻度および大きさと比較した当該製品の有用性、②損害発生の蓋然性および損害の深刻性、③製造業者また販売業者が当該製品を供給した時期、④合理的に予見し得る当該製品の用途および使用形態、⑤危険を防止するための設計・表示などの技術的・経済的実現可能性、⑥その他当該製品の安全に関連した事項などを総合的に考慮しなければならず、必ずしも、製品の絶対的な安定性を要求するものではない。

D．責任主体

製造物責任法は、製造の欠陥による損害に対して賠償責任に問われる者を「製造業者」

と規定している（製造物責任法第 2 条第 3 号)。「製造業者」としては、①製品を直接的に製造・加工した者と、②製品を直接的に輸入した者が中心となる。勿論、輸入品については、当然に直接、外国で製品を製造・加工した者に対しても損害賠償を請求することができる。

また、PB 商品や OEM 商品のように、直接製品を製造・加工しなくても、製品に商品名・商号・商標その他の表示をし、自己を製造業者・加工業者・輸入業者として表示し、もしくは誤解を招く表示をしている者も製造業者とみなされ、本法により責任を負わなければならないというのが一般的な解釈論である。

E. 損害賠償責任

製造物責任法において損害賠償とは、製造者が欠陥のある製造物により生命、身体また財産上の損害を受けた者に対して、その損害を賠償する責任を問うことをいう（製造物責任法第 3 条第 1 号)。製造業者は欠陥と相当因果関係がある全ての損害に対して賠償しなければならない。被害者は製品の欠陥で生命を失ったり、身体、健康を害した場合は勿論、財産の被害を受けた場合、損害額の多少を問わず、全ての損害に対して賠償を請求することができる。

製造物責任は現行民法第７５０条の不法行為責任の「故意また過失」の要件を「欠陥」によって置き換えたものである。民法上の不法行為責任においては、被害者が損害賠償を請求しようとすれば、製造者の故意また過失を立証しなければならない。

しかし、製造物責任においては、無過失責任を採択した。その理由は、産業社会の急激な発展により、製品が高度化・専門化する反面、被害を受けた消費者は製造工程および使用方法などに関する情報が足りないため、損害賠償請求のための要件事実の立証が難しくなったからである。そのため、製造物の欠陥・損害、そして欠陥と損害との因果関係だけ立証するようにし、消費者の負担を軽減したのである。

最後に、本法による損害賠償責任を排除したり制限しようとして、製造業者および販売業者と消費者の間で締結した契約は無効である。これは、製造業者などがあらかじめ自己の責任を制限する特約を約定しても効力がないようにすることで、消費者を保護するためである。但し、被害者が事業者の場合、人間の生命、身体ではなく、営業用資産に対して発生した損害について、製造業者と被害者間で締結した免責特約の効力は、例外的に認められている（製造物責任法第 6 条)。

F. 連帯責任

同一の損害に対して賠償する責任がある者が２人以上の場合は、各自が連帯してその損害を賠償する責任がある（製造物責任法第５条)。即ち、部品の欠陥により損害が発生した場合、部品製造業者と完成品製造業者が連帯して責任を負うことになる。連帯責任において被害者が誰に損害賠償を請求するかは自由で、実際上は、最も財力がある者を選択することになる。

まず賠償をすることになった者は、他の連帯責任者に対して内部的な責任比率に基づき求償権を行使することができるが、他方に支給能力がなければ、まず賠償した者が負

担を甘受しなければならない。

G. 製造者などの免責

製造物責任は絶対責任では無いため、製造物に欠陥があった場合であっても、一定の事由に該当し、製造者がこれを立証した場合には、製造物責任に基づく損害賠償責任責任を免れることができる（製造物責任法第 4 条)。但し、これは製造物責任法においての責任を免除するという意味であり、民法やその他の法律による賠償責任まで免除するものではない。

製造者の免責事由を見てみると次の通りである。

①製造者が当該製品を供給していない事実（製造物責任法第 4 条第 1 項第 1 号)。盗まれた製品のように、製造業者がその製品の供給に関与しない製品に関して被害が発生した場合が、これに該当する。

②製造業者が当該製品を供給した当時の科学・技術水準では、欠陥の存在を発見することができなかった事実（製造物責任法第 4 条第 1 項第 2 号)。これはいわゆる、「開発危険の抗弁」を規定したもので、開発上の危険に対して損害賠償責任を認めると、研究開発や技術開発が低迷し、究極的に消費者に損害を与えることになるのを考慮したものである。製造業者がこの開発危険の抗弁を主張し、責任を免れるためには、当該製品の欠陥の有無の判断に必要となる、入手可能な最高水準の科学・技術の知識に照らしても、欠陥を認識できなかったことを証明することが必要である。

③製造業者が当該製品を供給する当時の法令に定めてある基準を遵守したにもかかわらず、製造物の欠陥が発生した事実（製造物責任法第 4 条第 1 項第 3 号)。しかし、「KS」マークや「品」、「検」字マークなど、安全関連マークを受けたとか、形式的承認などを受けた事実だけでは、製造業者は責任を免除されない。

④原材料、部品の場合は、当該原材料や部品を使用した製品製造業者の設計または製作に関する指示により欠陥が発生した事実（製造物責任法４条第 1 項第４号)。これは原材料、部品製造業者だけに適用される免責事由である。しかし、このような免責事由が認定されたとしても、製造業者が製品を供給した後に製品に欠陥が存在する事実を知ったか、もしくは知ることができたにも関わらず、その欠陥による損害の発生を防止するための適切な処置を講じなかったのであれば、本法による責任の免除を受けることはできない（製造物責任法第４条第２項)。

H. 製造業者の責任期間（消滅時効など）

期間の経過により製品生産に関する各種記録や証拠が消滅すると、訴訟時に被告（製造者）の防御が困難になり、無限に潜在的な責任追及が続くことになると、製造者の合理的な製品開発計画や経営計画の樹立が難しくなる。したがって、損害賠償責任が永遠に存続することを防止し、製造者の法的安定性を確保する見地から、一定の期間が経過すると損害賠償請求の権利を否定する必要がある。現行民法上、不法行為責任においては、一定の期間が経過した際には損害賠償請求権を行使することができなくなり、製造物責任においても損害賠償請求権の消滅時効を認めている（製造物責任法第７条)。

?損害ならびに製造者などを知ってから３年（製造物責任法第７条第１項）

製造物責任の損害賠償は、被害者またその法定代理人が損害ならびに損害を発生させた製造者を知った時から３年以内に請求しなければならない。したがって、３年が経過した場合、損害賠償請求権は時効で消滅となる。このように時効期間を設けたのは、傷害または損害が発生し、被害者側は製造者に対して損害賠償を請求できる権利があるにもかかわらず、その権利の上に眠ることと、製造者が無期限に損害賠償を請求されることを防止するためである。

②製造者などが製造物を供給した日から１０年（製造物責任法第７条第２項）

製造者が損害を発生させた製造物を供給した時から１０年が経過した際には、損害賠償請求権が消滅する。例外的に、この期間は、身体に蓄積された場合に人間の健康を害する物質による損害、または一定の潜伏期間が経過した後に症状が現れる損害、例えば医薬品や化学製品のように、その服用または使用から被害発生まで長い時間がかかる場合などには、その損害が発生した時から起算することになる。製品が市場で使用されている限り、いつでも製造者は製造物責任を負担する危険を引き受けることになるので、このような製造者の不安定を解消するために、製品は製造また販売されてから一定期間が経過すると、それ以降は製造者や販売者を一切の賠償責任から解放する制度が置かれることとなった。

Ｉ．本質問と関連事項

情報セキュリティと関連して、欠陥があるハードウェアまたはソフトウェアの製造者が、製造物責任法に基づいて製造物責任を問われるのか否かについて考察してみる。

まず、ソフトウェアの場合を見ると、ソフトウェアが製造物責任法上の製造物の概念に含まれているかについて、多くの論議がある。上記で明らかにしたように、製造物責任法の対象となる製品は、「他の動産や不動産の一部を構成した場合を含む、製造また加工された動産」と規定されているので、まず、動産でなければならないことは明らかである。動産には有体物以外に、形態がない電気とその他管理できる自然力も含まれているが、例えばソフトウェアが有形的な媒体で固定された状態ではなく、オンラインを通して無形の情報だけで移転する場合には、このような無形的情報形態のソフトウェアが電気・その他管理できる自然力に該当するとみなすことができないので、製造物責任法の対象になり得ないことが比較的に明白だと判断される。しかし、ソフトウェアがCD-ROM パッケージ形態に固定された状態で販売された場合は、見解が分かれる可能性がある。現在、韓国で訴訟が提起されている SQL-Slummer 事件の場合、原告代理人は、SQL　Server プログラムの製造者であるマイクロソフト社を共同被告として訴訟を提起しながら、それが CD－ROM形態で販売され、動産に該当するとの理由で、基本的に製造物責任を問い、補完的に不法行為責任を問うという方式で、請求原因を構成した（添付資料#9、#10、#11 参照）。

ハードウェアの場合は、動産に該当することに疑問がないため、製造物に該当するかをめぐっての論難は起きないものと予想される。

製造物に該当することに問題がない場合は、結局、その欠陥が製造物責任法でいう欠陥に該当し、被害者らが受けた財産上の損害が、その欠陥と相当因果関係にあるか否か

が重要な事項として取り扱われることとなろう。

２．刑事責任など

（１）情報通信基盤保護法の規定

情報通信基盤保護法では、重要通信基盤施設に対する電子的侵害行為と関連して、次のような刑事処罰規定と過料規定を設けてある（条文内引用条文などは添付資料#１参照)。

①重要情報通信基盤施設撹乱などの行為に対する処罰（法、第２８条）

次の行為を行い、重要情報通信基盤施設を撹乱、麻痺また破壊した者は１０年以下の懲役また１億ウォン以下の罰金に処する。

１．アクセス権限を持たない者が、重要情報通信基盤施設へアクセスしたり、アクセス権限を持った者が、その権限を越えて保存されたデータを操作・破壊・隠匿また流出する行為

２．重要情報通信基盤施設に対してデータを破壊したり、重要情報通信基盤施設の運営を妨害する目的でコンピュータウィルス・論理爆弾などのプログラムを投入する行為

３．重要情報通信基盤施設の運営を妨害する目的で、同時に大量の信号を送ったり、不正な命令を処理させるなどの方法で、情報処理に間違いを発生させる行為

上記の規定において情報通信基盤施設とは、国家安全保障・行政・国防・治安・金融・通信・運送・エネルギーなどの業務と関連する電子的な制御・管理システムおよび「情報通信網利用促進ならびに情報保護などに関する法律」第２条第１項第１号の規定する情報通信網をいう（上記、法、第２条第１号参照；

一方、「情報通信網利用促進及び情報保護に関する法律」第２条第１項第１号には、「『情報通信網』とは、電気通信基本法第２条第２号の規定により、電気通信設備を利用したり、電気通信設備とコンピュータおよびコンピュータの利用技術を活用して、情報を収集・加工・保存・検索・送信また受信する情報通信体制をいう。」と定義している）。

結局、インターネットなど、情報通信網自体が情報通信基盤施設に含まれるということが分かるが、上記の処罰規定はその中でも「重要」情報通信基盤施設（重要情報通信基盤施設の指定に関連しては同法第８条参照）を撹乱、麻痺、破壊した場合を適用対象とし（結果的加重犯）、続いて２号、３号の場合の重要通信基盤施設の運営を妨害する目的を要件とすることで(目的犯)、以下の論述からも分かるように、一般的なコンピュータウィルス流布などの行為に比べて、かなり加重された刑罰を科している。

②秘密漏洩に対する処罰（法、第２９条）

第２７条の規定に違反して秘密を漏洩した者は５年以下の懲役、１０年以下の資格停止また５千万ウォン以下の罰金に処する。

③過料（法、第３０条第１項）

次の各号の何れかに該当する者は１千万ウォン以下の過料に処する。

１．第１１条第１項の規定による保護処置命令に違反した者

２．第１６条第２号の規定による通知をしていない者

３．第２０条の規定による申告をしていない者

４．第２２条第２項の規定を違反して、関連書類また資料を提出していないか若しくは

虚偽に提出した者
５．第２３条第２項の規定を違反して、記録及び資料を返還するか若しくは廃棄していない者

（２）情報通信網利用促進ならびに情報保護に関する法律の規定

情報通信網利用促進ならびに情報保護に関する法律では、一般的な情報通信網を侵害する行為などに対して、次のような処罰規定を設けている（法律全文は添付資料#５参照)。

?　情報通信網を侵害する行為等
正当なアクセス権限なしに、あるいは許容されたアクセス権限を越えて情報通信網に進入した者は、３年以下の懲役または３千万ウォン以下の罰金に処する（情報通信網利用促進ならびに情報保護に関する法律、第６３条第１号、第４８条第１項)。
正当な事由なしに情報通信システム、データまたプログラムなどを毀損、滅失、変更、偽造し、または、その運用を妨害できるプログラム（悪性プログラム）を伝達または流布した者、情報通信網の安定的な運営を妨害する目的で大量の信号またデータを送り、もしくは不正な命令を処理させるなどの方法で情報通信網に障害を発生させた者は、５年以下の懲役また５千万ウォン以下の罰金に処する（上記、法、第６２条第４号、第４８条第２項、第６２条第５号、第４８条第３項)。

② 情報毀損、秘密侵害
情報通信網によって処理、保管また転送される他人の情報を毀損したり、他人の秘密を侵害､盗用また漏洩した者は５年以下の懲役また５千万ウォン以下の罰金に処する(情報通信網利用促進ならびに情報保護に関する法律、第６２条第６号第４９条)。

（３）刑法上の規定

①コンピュータに関連する業務妨害
コンピュータなど情報処理装置また電子記録など特殊媒体記録を損壊し､もしくは情報処理装置に虚偽の情報または不正な命令を入力したり、その他の方法で情報処理に障害を発生させ、その業務を妨害した者は５年以下の懲役、または１千５百万ウォン以下の罰金に処する（刑法、第３１４条第２項)。
ウィルスを侵入させる行為、メール爆弾またスパムメールなどでシステムに過負荷を招来する行為、正常な命令語を使用してサービスを過度に要請するサービス拒否攻撃行為（Denial of Service　Attack, DOS Attack）､インターネットを転々としてシステムの性能を低下させるインターネットワームを流布させる行為、一定の条件が充足されるとシステムを破壊する論理爆弾を使用する行為などと共に、電話交換機システムを撹乱させるフォンプレーキング(Phonephreaking)も本罪に該当する事例とされている。

②秘密侵害
封緘、その他の秘密の処理をした人の手紙、文書、図面または電子記録など特殊媒体

記録を、技術的手段を利用して、その内容を調べ出した者は、３年以下の懲役また５百万ウォン以下の罰金に処する（刑法、第３１６条第２項）。

3.2.2：法的責任の要素(Elements of security legal liability)

情報セキュリティ、機密性、正確性、可用性と法的責任には、どのような関係がありますか[IT6]。

【回答】質問の趣旨を正確に理解することが困難であるが、結局、過失の可否を検証するときに、どのような注意義務があったかということが重要な判断要素になることが上記で明らかになったのであって、その注意義務と関連して情報セキュリティの機密性などいろいろな状況が具体的、個別的に考慮されると考えられる。

3.2.3: 主体的側面(Subjective aspect)

情報セキュリティに対する侵害があった場合に、被害者から責任を追求され得る当事者についてあげて下さい。
具体的に[IT7]以下の例について記述して下さい。

【回答】

・ハッカー(脆弱性に対して攻撃するソフトウェアを開発し、意識的に配布する者)：
民事的には故意の不法行為を行った者と評価され、被害者などがそれに基づいて被ることになるあらゆる損害を賠償しなければならない。刑事的には状況により上で見たところと同じく、刑法上のコンピュータに関連する業務妨害罪、電子通信網利用促進ならびに情報保護に関する法律上の情報通信網侵害行為などに該当し、それに従って処罰され、されにそれが重要情報通信基盤施設を撹乱、麻痺または破壊する結果をもたらす場合には、情報通信基盤保護法上の処罰規定に抵触し、それに従った重い処罰を受けることになる。

・ 脆弱性の存在するハードウエアまたはソフトウエアの製造業者または開発者
特別な場合を除いては､刑事責任は問題にならず､民事責任の有無のみ問題となろう。上で見たところと同じく、ハードウェアの場合は製造物責任法上の「製造物」に該当することに疑問はなく、そのハードウェアの欠陥によって被害を受けた者は製造物責任法に基づく損害賠償を請求できることになろう。ソフトウェアの場合には、無形的な情報自体のみでは製造物ということはできず、製造物責任法の適用対象ではなく、それをパッケージして CD－Rom など有形的媒体に保存し、流通させた場合にも、故意または過失で欠陥（脆弱性）があるソフトウェアなどを製造、販売して他人が被害を受けたと認定されれば､民法上の不法行為責任を負う場合があり得る｡また、製造者から商品を直接、購入した者との関係では、欠陥のある製品の引渡しが不完全履行であるという理由で、債務不履行責任を負わなければならない場合がある。さらにそのソフトウェアなどに瑕疵があり、その瑕疵の存在事実を購入者が知らず、知らないことに過失がなかった場合には、民法上の瑕疵担保責任を問える場合もあり得よう。但し、一般的な債務不履行責任であれ、瑕疵担保責任を問い得ることは直接的な契約当事者に限られ、他の第三の被

害者はこうした主張をすることはできない。

・ コンサルタント、システムインテグレーター、配布者、販売業者、その他脆弱性のある技術を推奨したベンダー

脆弱性のある技術を推薦したコンサルタントなどがその技術を導入した側との間で、一定の対価のもとにコンサルティング業務を適正に遂行する契約を締結しているのに、こうした契約上の義務を負担していて、その義務を適正に履行していないものと認定され、契約の相手方がそれに基づき損害を被った場合であれば、その相手方に対して、債務不履行責任を負わなければならない。他の第三者である被害者に対しては、彼らに対する一般的な注意義務を欠く故意、過失が認定される場合に限り、民事責任が問題となり得る。

・ セキュリティの評価やセキュリティ脆弱性の回避を委任されたコンサルタント

この場合、コンサルタントがセキュリティの評価を誤り、セキュリティの脆弱性を回避する義務を十分に履行しなかったか、履行しなかったことにより、委任者側が損害を受けた場合には、債務不履行責任を負わなければならない。場合によっては、一般的な故意、過失が認定される場合には、第三の被害者たちに対しても、不法行為責任を負わなければならない場合があり得る。

韓国では、スラマーに関連して提起された訴訟では、大韓民国（情報通信部）が共同被告のひとりになっているが、これは、重要情報基盤施設を管理する機関の長（この事件では情報通信部長官）が、この基盤施設の脆弱性を分析し、回避するための措置をとる法令上の包括的義務を負担しているという点を前提としたものである。もちろん、この事件では、原告が勝訴するためには、情報通信部が実際の法令上の注意義務に違反していたということと、それと被害者たちが被った損害との間に相当因果関係があるということを主張、立証しなければならない。事件はまだ、準備手続きの段階である。

・ 脆弱性を発見する監査人

この監査人は、脆弱性を発見すれば、即座にこれを回避するための措置をとらなければならない契約上の義務を負っているが、これを履行しなかったことにより被害を惹起した場合であれば、契約上の債務不履行責任を負わなければならず、こうした義務を法令または社会常識（条理）によって負担している場合では、不法行為責任を負う場合があり得る。

・ 攻撃を抑止するように依頼していたセキュリティ・プロバイダー

契約によって依頼をうけたセキュリティ・ロバイダーが、契約上の義務を十分に履行しなかった場合には、契約上の債務不履行責任を負うことになり、彼らが対外的な面でも故意、過失があることを認定された場合には、第三の被害者たちに対する関係でも、不法行為責任を負うことになる場合があり得る。

・ アプリケーションを最新に、パッチを当ててもらうことにしているアプリケーション・サービスプロバイダー

ASP サービス提供会社が、ソフトウェアの脆弱点を保管するパッチファイルを当てずに、ハッキングなどの攻撃を受けた場合には、原則的にそのサービス利用者に対する関

係で債務不履行責任を負わなければならない可能性が高く、過失に基づく不法行為責任も免れるのは難しい場合が多い。

・ システムをアウトソースしている場合のホスティング会社
　システムをアウトソーシングしている場合であっても、ホスティングサービスの顧客に対する関係では、アウトソーシングしているという理由だけで債務不履行責任を免れることはできない。不法行為責任の有無を判断するにあたっては、前述した一般的な原則の他に、使用者責任の有無に関する法的判断が必要になる。これに対する韓国の法制度は、日本の場合とほぼ一致する。

・ 攻撃を許容し、または、停止し得なかった ISP
　上記で、「下流責任」と関連して説明した部分を、この部分に対する回答に代えることができよう。
　具体的な状況に従い、個別的に注意義務違反の有無を判断しなければならず、後で説明する、「情報通信サービス情報保護の指針」が注意義務の有無を判断するにあたって、重要な参考になる法規上の基準であるということができる。この指針によると、その注意義務は、侵害事故の予防に関する注意義務と、侵害事故発生時の迅速で適切な対処に関する注意義務に分けられる。

・ （追加）IDC センター
　韓国の「情報通信網利用促進ならびに情報保護に関する法律」第４６条によれば、「①他人に情報通信サービスを提供するために集積された情報通信施設を運営、管理する事業者は、情報通信施設の安全な運営のために、情報通信部令が定めるところにより、保護措置をとらなければならない。
　②第１項の規定による事業者は、集積された情報通信施設の滅失、毀損、その他運営の障害によって発生した被害を補償するために、情報通信部令が定めたところに従い、保険に加入しなければならない。
　③情報通信部長官は、第１項の規定による保護措置をとらない事業者に対し、相当な期間を定め、是正措置を命ずることができる。」と、規定している。いわゆる、サーバの賃貸を業としている IDC センターの場合、上記のような保護措置をなおざりにして事故が発生した場合には、それに従って、債務不履行ならびに不法行為責任を負わなければならない。

・ 脆弱性を発見していながら、それを被害者、ベンダーまたは公に報告しなかった者
　報告しなかったすべての人が法的責任を負うのではない。契約上、明示的にあるいは黙示的に、報告義務を負っている場合には、契約上の債務不履行責任を、法令または条理上の報告義務が認定される場合には、債務不履行責任を負うことになる場合がある。
　韓国の情報通信基盤保護法では、情報保護コンサルティング専門企業に対して、一定の保護義務ならびに記録保存などの義務を賦課している（同法、第２２条、第２３条など参照)。情報保護コンサルティング専門企業がこうした法令上の義務に違反したことが侵害事故の原因である場合には、不法行為などの責任を負う場合があり得る。

3.2.4. 脆弱性の場所

以下のような脆弱性の発生個所によって、責任を問われる人が異なりますか？
- クライアント側
- サーバ側
- ネットワーク機器部分
- など

【回答】これに関する特別な規定があるわけではないが、民法などの一般原理を適用して責任主体による責任の有無、特に注意義務違反の有無を検討するに当たって、上記のような脆弱性発生位置の問題は、かなり重要な要素となるであろう。クライアント PC において脆弱性が発生したら、サービス提供者側に責任を問うことは難しい場合が多いであろう。サーバ側に脆弱性があるのなら、これを利用し、顧客にサービスを提供する会社ならびに関連ハードウェアの製造者などの責任が問題になるし、ネットワーク機器部分に脆弱性があれば、機器製造者や納品業者側の責任が問題となる外に、その機器を利用してインターネット接続サービスなどを提供している会社側に責任がある可能性が多いであろう。

以下のようなソフトウェアの提供形態によって、責任の違いを区別しているかを解説してください。
- パッケージ品ソフトウェア（市販品）
- 個別開発品ソフトウェア
  - 外注（成果物検収 Deliverable）
  - 委託（工数検収 Labor hour）
- サービス提供に利用しているソフトウェア
- など

【回答】やはりこれに対する特別な規定は別にあるわけではなく、民法などの一般原理に基づいて判断しなければならない。上記で明らかにしたように、パッケージ商品中に、有形的な媒体（動産）に固定された形態で提供された場合には、製造物責任法の適用対象になり得るという主張があるが、これに対して、まだ判例が出たことはない。もし、これが判例によって承認されたら、製造物責任法の適用の可否と関連して、CD などの有形的な媒体に固定されたパッケージ形態の販売と、そうではない場合とでは、かなりの違いが生じることになるであろう。

3.2.5 注意義務－標準(Duty of care-standard)

3.2.5.1 一般(general)

法によって情報セキュリティの基準が定義されていますか。
脆弱性の改善義務についての基準を法令等で設けていますか？
法令等以外の情報も知っていれば教えてください。

【回答】情報通信網利用促進ならびに情報保護に関する法律（及び同法施行令、施行規

則）に、情報通信網における情報保護に関する一般的な規定を置いている（上記、法律および施行令、施行規則全文は添付資料#５、#６、#７参照)。

上記、情報通信網利用促進ならびに情報保護に関する法律第５２条第１項は、「政府は情報の安全な流通のため、情報保護に必要な施策を効率的に推進するために、韓国情報保護振興院（KISA）を設立する。」と規定し、同条第３項において、KISA の業務を規定し、その中の一つに、＜情報保護システムの性能と信頼度に関する基準制定ならびに標準化支援＞を揚げている（同項第５号)。

また、上記、法第４７条第１項は、「情報通信サービス提供者および情報通信サービスを提供するために物理的施設を提供する者は、情報通信網の安定性および情報の信頼性を確保するために樹立運営している技術的・物理的保護処置を含む総合的管理体系（以下、「情報保護管理体系」と呼ぶ）が、当該サービスに適合するか否かに関して、第５２条の規定による韓国情報保護振興院から認証を受けることができる。」と規定し、情報保護管理体系認証制度を設けている（２００１．７．１．施行)。

上記規定によって韓国では、KISA の主導で情報保護に関する標準の制定ならびに認証業務を遂行している。

特に情報保護管理標準（TTAS.IS-17799）は、「情報保護管理体系認証制度」の基礎となるもので、国際標準 ISO/IEC 17799 を応用して、韓国情報保護振興院（KISA）が国内実情に合うように開発したものであり、それまで適切な保安管理指針書がないために業務遂行に難しさを感じてきた保安管理者は勿論、認証審査機関の業務遂行について指針書の役割を果たすことを期待されている。

3.2.5.2. 管理者の義務[IT8] (Duties of administrators)

システム管理者が、不具合を修正するためになすパッチやソフトウェアを使用することを怠った場合、責任があるか。

システム管理者がセキュリティ情報を収集するのを怠ったとき、責任があるか。

【回答】「情報通信網利用促進ならびに情報保護に関する法律」第４５条第１項は、「情報通信サービス提供者は、情報通信サービスの提供に使用される情報通信網の安定性および情報の信頼性を確保するために、保護処置を準備しなければならない。」と規定し、同条第２項は、「情報通信部長官は、第１項の規定による保護処置の具体的な内容を定めた情報通信サービスの情報保護に関する指針を定め、公示して、情報通信サービス提供者にその遵守を勧告することができる。」と定めていて、この規定による情報通信サービスの情報保護指針が情報通信部により公示されている（添付資料#８参照)。

このような規定により、全ての情報通信サービス提供者は、情報通信網の安定性および情報の信頼性を確保するため、保護処置を準備する法的義務があり、その具体的な保護処置については、上記指針に規定された内容が一つの基準として適用されるであろう。少なくとも注意義務の有無を判断するにあたって、上記の指針は重要な基準として働くものであろう。ところで、上記指針によると、情報通信サービス会社は、システム管理者と情報保護責任者を指定しなければならないし、情報保護責任者は脆弱性に対して周期的な点検、分析および報告義務を負っている。このような義務の内容には、保安脆弱

性に対するパッチプログラムが出たという情報を適時に入手して、これを活用すべき義務も含まれているものと解釈されるので、これを怠った場合には、注意義務に違反したことになり、相手によって、不法行為または債務不履行責任を問われる可能性が高いであろう。

3.2.5.3 インシデントにおけるシステム管理者の義務（Duties of system administrators in case of incidents）

インシデントに対応する際、システム管理者は、不十分な対応しかできなかった場合、または、対応がおくれた場合、責任を負うか。

損害を回避する責任を負う当事者が他にいますか。

【回答】これは情報セキュリティに対する侵害事故を予防するための注意義務ではなく、侵害事故発生時の適切な処置に関する注意義務に関連するものである。情報通信サービス情報保護指針第８条第５項によると、サービス提供会社により指定された情報保護責任者は、周期的にアクセス記録を分析して侵害事故を予防し、侵害事故を発見した場合には直ちに必要な処置を取らなければならないと規定されている。この中で、後半部分がこれに該当する。情報保護責任者が直ちに必要な処置を取らなければならないという注意義務を怠ったことにより、顧客などに被害が発生し、または拡大した場合には、情報通信サービス会社としては、債務不履行責任と共に、不法行為に対する使用者責任に基づいて損害賠償義務を問われる場合が多いであろう。侵害事故時の対応が一見不十分に見えても、現在の技術水準としては、それ以上の対処が不可能な場合であれば、注意義務が認定される範囲を超える場合として、責任を免れることになるであろう。

情報保護責任者が被用者の場合には、契約責任は会社自体が負担し、不法行為責任は会社と担当責任者が不真性連帯責任を負うことになろう。

この他に、情報保護業務を第三者に依頼した場合にも、契約責任は依頼した会社にあり、不法行為責任は依頼を受けた会社が問われる場合が多いであろう。

3.2.5.4. セキュリティ・ポリシー(Security policies[1])

１　注意義務の標準として、セキュリティポリシーを必要としていますか。

【回答】注意義務の基準となる情報保護基準は必要なものと認識されており、上述のように、「情報通信サービス情報保護指針」が制定されている。

２　保険会社や産業界の事業者協会で、ガイドラインを標準としていることはないですか。

【回答】政府および傘下機関の法規、指針以外に産業会のガイドラインは発見できなか

[1] In this context,” security policies” have broad meaning and include “Implementations, Planning and Audit”cycle.

った。

３　セキュリティポリシーの実際の運用が責任に対する抗弁になりますか。

セキュリティポリシーの実際の運用が、連邦ガイドライン[IT9]のようにコンプライアンスの観点から考えられていますか。

【回答】情報保護業務の法規の基準を遵守したのであれば、債務不履行責任に関連して帰責事由がないと抗弁するにあたって大きな助けとなり、不法行為に関連しても法規上の注意義務は遵守したものと認定される可能性が高いと思われる。事業者が自主的に作ったセキュリティポリシーがある場合、これは法規上の基準に照らして正当性が認定される場合に限って、このような効力があると思われる。

４　セキュリティ上の脆弱性が、セキュリティの監査および評価をしていながら、それを探知できなかった場合、その監査および評価をしていた事実は、抗弁となりえますか。

【回答】「情報通信サービス情報保護指針」第８条第４項においては、「情報保護責任者は、周期的に情報システムの保安脆弱点を点検、分析して、その結果を情報通信サービス提供者に報告しなければならない。」と規定されているので、情報保護責任者が情報システムの保安脆弱点を周期的に点検、分析しているのであれば、これ自体が上記指針上の（注意）義務を遵守している部分であり、損害賠償請求訴訟において有力な抗弁事由の一つとなり得る。しかし、通常の情報保護責任者であれば十分にその脆弱点を探知することができたのにも関わらず、これを行っていない場合には、過失が認定され、債務不履行または不法行為責任を免れ得ない可能性が高い。

3.2.6 その他[IT10](Miscellaneous)

１　セキュリティ・インシデントの実体を明らかにするのに有効だと考えられる法的システムはありますか。

【回答】公共機関が持っている情報に対しては、公共機関の情報公開に関する法律において、一般国民に「情報公開請求権」を認める規定が設けられている。この法律に対して市民団体などでは、まだ情報公開の範囲などが微弱であるとして、全面的な改正を主張している。その他 ISP、重要ソフトウェア製造者などに対しては、情報公開請求制度が認められておらず、ただ民事訴訟が提起される場合に「文書提出命令」の申請などにより、一定の情報の提出を強制し得る方法があるにすぎない。

逆に、情報通信部など政府機関の立場は、事故の実態を素早く把握するため、ISP が持っているログ資料などの提出を要求する権利を持ちたがっている。韓国における SQL-Slummer 事件が発生した後、情報通信部では、このような方向の立法を推進しようとの意見がもちあがり、これに対してプライバシー侵害を警戒する市民団体の強い反対意見が提起された事がある。

２　「内部告発者保護」や「司法取引」の法制度を有していますか。

【回答】最近、韓国の政府（財政経済部）は、会計情報に対する企業の責任を強化する法案として、公示書類（公用文書）虚偽記載を指示した場合に、関連した内部告発者保護規定を導入するという方針を明らかにしている。尚、法務部は、権力型非理（不祥事）剔抉（暴き出すこと）のための腐敗監視システムの一環として、内部告発者の身分保障、申告者の免責などを制度化するという方針を明らかにしている。しかし、また推進段階であり、具体的な立法成果が表われているわけではない。上記のような会社支配構造および、権力型不祥事に関連した問題の他に、一般的な内部告発者保護制度の必要性は、市民団体を中心として提起されているが、いまだに確かな結論が出ていない。情報保護に関連した内部告発者保護制度については、いまだに韓国では大きく論議されてはいないものと思われる。

アメリカの法廷映画でよく見られる「司法取引」は、韓国国民感情には合っていないと考えられるし、これに対しては導入論議が全く見られない。

３　「内部告発者保護」や「司法取引」の法制度が、セキュリティ・インシデントの実体を明らかにするのに有効と考えられるのではないかという議論はありませんか。

【回答】韓国で上記の二つの項目は、上で述べたように情報保護問題に関連しては、特別な論議の焦点にはならなかった。

3.3 責任ある開示の問題[IT11](Responsible disclosure issue)

１　脆弱性に気がついたとき、気がついた人間は、会社や公的機関に報告すべき義務がありますか

【回答】「情報通信サービス情報保護指針」第８条第４項は、「情報保護責任者は、周期的に情報システムの保安脆弱点を点検、分析して、その結果を情報通信サービス提供者に報告しなければならない。」と規定している。

その他に公的機関に報告する義務を規定している法規はいまだにない。後で詳しく紹介する情報通信網利用促進ならびに情報保護に関する法律改正案には、上記のような報告義務を拡大する規定が含まれている。

２　報告された会社などは、これに対して対応すべき義務はありますか。また、対応をなしうる体制をとっておく義務があると解されていますか。

【回答】「情報通信網利用促進ならびに情報保護に関する法律」および、それに基づく、「情報通信サービス情報保護指針」によると、このような対応義務および管理体制構築義務があると解釈される。

このような部分も、後で紹介する情報通信網利用促進ならびに情報保護に関する法律改正案において、より強化された形の義務規定に変っている。

３　産業界や政府の機関が、脆弱性がわかった際に、それに対して責任ある開示となるようなガイドラインを準備していますか。もし、準備している際は、その内容をお教えください。

【回答】責任ある公開に関連した議論は、韓国であまり見られないようである。但し、情報通信基盤保護法においては、中央行政機関の長と、長から委任を受けた管理機関の長が、重要情報通信基盤施設の脆弱点の分析、評価、対処などに関連して、組織的、行政的支援のいろいろな処置および方案を講ずることができるよう、根拠規定を設けている（添付資料参照）。

４　脆弱性の報告について、その内容を分析する専門的な委員などの制度が提案されていませんか。もし、議論されているのであれば、その内容をお教えください。

【回答】情報通信基盤保護法第９条においては、重要情報通信基盤施設に対する脆弱点の分析、評価に関連して、「専門チーム」を設ける根拠規定を準備している。その他には、別の論議についてはわからない。

3.4 SQL Slummer の事件をきっかけに何か動きなどがありましたか？

【回答】韓国情報通信部においては、最近、いわゆる「インターネット大乱」（SQL-Slummer 事件）を契機に、情報保護関連規定を大幅に強化することを重要内容として含んだ、情報通信網利用促進および情報保護に関する法律改正案を出し、公聴会などを通して世論を収斂している。その内容は次の通りである（添付資料中の「情報通信網法改正関連資料.hwp」参照）

Ａ．改正の背景

o　情報化の進展により、各社会部門がネットワークで相互連結され、政府、企業、その他団体および個人の活動は、情報システムとネットワークに絶対的に依存している。

-　しかし、情報システムとネットワークにより保存、伝達される情報は、非認可アクセスによる使用、誤用、変造、悪性コード転送、サービス拒否またはシステム破壊のような多様な危険にさらされている。

o　特に、去る１月２５日のインターネット侵害事故は、従前のサイバー攻撃と異なり、ネットワーク自体を攻撃し、急速にインターネット網全体に障害を発生させる新たな形態に変化した。

-　いまや情報保護は特定な部門の問題ではなく、情報システムとネットワークを利用する政府、企業、利用者全体の問題に拡大し、皆が総体的に協調してこそ、効果的な対応が可能である。

o　また、最近、個人情報管理が杜撰なために流出する事例が発生するなど、個人情報保護に対する不安感が大きくなり、個人情報保護を管理する処置の強化が必要となった。

o　したがって、インターネットの公共性を勘案し、インターネットの安全性、信頼性を確保して、インターネットを利用する各利用者の責任と役割を提高する（高める）ため、関連法律の改正を推進する。

B.　経過および重要内容

1）推進経過

o　2003.3.13　：情報通信網保護対策政策討論会開催
　-　重要政策法案発表、および関係専門家などからの意見収斂

o　2003.3.28　：大統領年頭業務報告
　-　インターネット侵害事故対応支援センター設置、情報保護事前評価制導入などを報告

o 2003. 4　：情報通信網保護対策新部計画樹立

o 2003. 5　：法律改正　専門作業チームの構成、および改正案初案の準備

　- 2003.5.27　重要内容を情報通信基盤保護実務委員会に報告

2）重要な改正の内容

□　侵害事故に関連する重要改正内容

o　インターネット侵害事故発生時における迅速な対応と原因分析

　-　インターネット侵害事故対応支援センターの設置とその役割

　-　ISP、IDC、アンチウィルス業者などに対して、侵害事故を迅速に報告するようにし、侵害事故原因分析などのために、ログ記録保存命令制、現場調査権、資料提出要求権などを規定した（これに対しては上述の通り、市民団体－一緒に動く市民行動－などからの、プライバシー保護の側面での強い批判に直面している）。

o　個人、企業、政府など各部門別に情報保護を強化する。

　-　現在、IDC だけに保護処置を義務化しているが、ISP、IDC、大衆利用施設などに対して細分化して、情報保護安全基準を賦課し、これを遵守するように義務化を規定した。

※情報保護コンサルティング専門業者などを通して周期的な安全診断を実施し、KISA の安全診断基準および技術開発、遠隔診断サービス提供などの業務を規定した。

- 情報通信施設が集中している IDC の場合、重大な侵害事故の発生時に、IDC が、入居している業者のサーバに対し、異常トラフィックの遮断などの緊急処置を行う権限などを付与した。

- ISP を通じた利用者情報保護処置の強化

- S/W 業者には、保安パッチ情報を購買者に２回以上告知させることとした。

o 情報保護投資拡大の推進

- 政府、地方自治団体などが一定規模以上の情報化事業を推進するとき、企画段階から情報保護要素を反映できるよう、「情報保護事前評価制」を導入した。

o ハッキング、ウィルス流布など、サイバー犯罪の処罰を強化した。

o その他情報保護産業、情報保護産業協会の根拠規定の準備など

（個人情報保護に関する改正規定についての紹介部分は省略する）

3.5 「ソフトウェアの脆弱性に対応するガイドライン」の観点でご意見があれば教えてください。

特別な意見はなし。
以上